



U.S. Department of Justice

**Federal Bureau of Investigation**  
*Washington, D.C. 20535*

November 18, 2016

MS. ALEXA O'BRIEN  
POST OFFICE BOX 6509  
ASTORIA, NY 11106-9997

FOIPA Request No.: 1340324-000  
Subject: FBI Campus Liaison Program

Dear Ms. O'Brien:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act. Enclosed is one CD containing 268 pages of previously processed documents and a copy of the Explanation of Exemptions. This release is being provided to you at no charge.

Based on the information you provided, we conducted an additional search of the locations or entities where records responsive to your request would reasonably be found, to include the Central Records System and any Electronic Surveillance (ELSUR) records. We were unable to identify additional records responsive to the FOIA.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

For questions regarding our determinations, visit the [www.fbi.gov/foia](http://www.fbi.gov/foia) website under "Contact Us." The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request. Your patience is appreciated.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's FOIAonline portal by creating an account on the following web site: <https://foiaonline.regulations.gov/foia/action/public/home>. Your appeal must be postmarked or electronically transmitted within ninety (90) days from the date of this letter in order to be considered timely. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS) at 877-684-6448, or by emailing [ogis@nara.gov](mailto:ogis@nara.gov). Alternatively, you may contact the FBI's FOIA Public Liaison by emailing [foipaquestions@ic.fbi.gov](mailto:foipaquestions@ic.fbi.gov). If you submit your dispute resolution correspondence by email, the subject heading should clearly state "Dispute Resolution Services." Please also cite the FOIPA Request Number assigned to your request so that it may be easily identified.

Sincerely,

A handwritten signature in black ink, appearing to read "D. Hardy", is written over the word "Sincerely,".

David M. Hardy  
Section Chief,  
Record/Information  
Dissemination Section  
Records Management Division

Enclosure(s)



## **EXPLANATION OF EXEMPTIONS**

### **SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552**

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information ( A ) could reasonably be expected to interfere with enforcement proceedings, ( B ) would deprive a person of a right to a fair trial or an impartial adjudication, ( C ) could reasonably be expected to constitute an unwarranted invasion of personal privacy, ( D ) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, ( E ) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or ( F ) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

### **SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a**

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.



FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1212788-0

Total Deleted Page(s) = 9

Page 3 ~ b7E;  
Page 64 ~ b7E;  
Page 65 ~ b7E;  
Page 66 ~ b7E;  
Page 67 ~ b7E;  
Page 68 ~ b7E;  
Page 69 ~ b7E;  
Page 70 ~ b7E;  
Page 71 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX



Campus Liaison Initiative  
**MISSION**

Continuously enhance liaison  
relationships with colleges and  
universities in an effort to  
increase mutual cooperation  
and information sharing  
between campuses and Joint  
Terrorism Task Forces (JTTFs)

to



*There is a Campus Liaison Agent (CLA)  
on the Joint Terrorism Task Force in  
every FBI Field Division dedicated to the  
success of this program. Please reach  
out to your local CLA.*

Visit our LEO SIG @ [www.leo.gov](http://www.leo.gov)

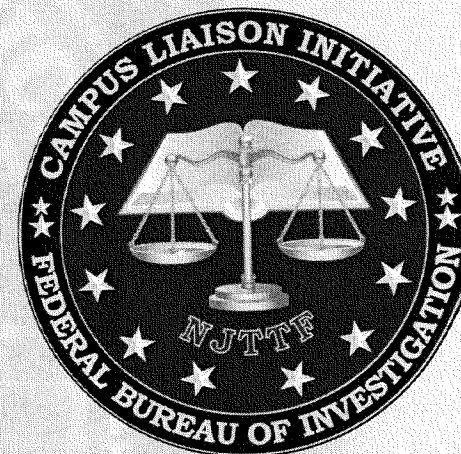
**Local FBI Campus Liaison  
Agent:**

Address:

Phone:

E-mail:

U.S. Department of Justice  
Federal Bureau of Investigation



**Campus Liaison  
Initiative  
(CLI)**

b7E



## Our Goal

- ♦ Establish a point of contact at each institution
- ♦ Create an information-sharing environment
- ♦ Operate within the guidelines of FERPA / Buckley Amendment
- ♦ Increase awareness and provide training for Campus Administrators and Public Safety personnel

*"People who act out violently don't wake up one morning and snap. There are clues."*

- FBI Supervisory Special Agent  
Behavioral Analyst



## Benefits of CLI

- \* Strong relationships based on trust prior to a crisis
- \* Increased two-way information sharing
- \* Raise awareness of campus vulnerabilities
- \* Provide awareness of ongoing threats and investigations
- \* Make campuses safer places to work, live and learn

## Balancing a Fine Line

- Heightened security contrasts with the role of colleges and universities as institutions where open access and free speech are fundamental.
- Balance is essential between two imperatives [REDACTED]

b7E

## Things to consider :

- Set up a secure campus information system for the campus community to report potential suspicious activity.
- Campus Public Safety should not hesitate to report information to their local JTTF
- Don't become complacent
- Ensure enhanced communication systems both within campus and with outside agencies
- Draft MOUs/Mutual Aid agreements with other area agencies
- Develop a campus Crisis Response Plan
- Liaison, train, and exercise your plan with other local/state/federal agencies





## Telephone, Laptop & PDA Security

If you can do without the device, Do Not Take It!

Do not leave electronic devices unattended. Do not transport them (or anything valuable) in your checked baggage. Shield passwords from view. Avoid Wi-Fi networks if you can. In some countries they are controlled by security services; in all cases they are insecure.

Sanitize your laptop, telephone, & PDA, prior to travel and ensure no sensitive contact, research, or personal data is on them. Back-up all information you take and leave that at home. If feasible, use a different phone and a new email account while traveling.



Use up-to-date protections for antivirus, spyware, security patches, and firewalls. Don't use thumb drives given to you – they may be compromised.

*During the Beijing Olympics, hotels were required to install software so law enforcement could monitor the Internet activity of hotel guests.*

Clear your browser after each use: delete history files, caches, cookies, and temporary internet files.

## Upon Your Return

Report any unusual circumstances or noteworthy incidents to your study abroad program manager and to the FBI. Notifying the FBI will help ensure that future travel advisories take into consideration the circumstances and incidents you encountered. It is not uncommon for foreigners to contact you after your return. The FBI may be able to help you determine if these contacts pose any risk to you.

### Important Numbers

US Embassy/Consulate Phone & Address:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

POC in country: \_\_\_\_\_

\_\_\_\_\_



In most countries, you have no expectation of privacy in Internet cafes, hotels, airplanes, offices,



or public spaces. All information you send electronically (fax, computer, telephone) can be intercepted, especially wireless communications.

If information might be valuable to another government, company or group, you should assume that it will be intercepted and retained. Security services and criminals can track your movements using your mobile phone and can turn on the microphone in your device even when you think it is turned off.

Beware of "phishing." Foreign security services and criminals are adept at pretending to be someone you trust in order to obtain personal or sensitive information.

If your device is stolen, report it immediately to the local US Embassy or Consulate.

Change all your passwords including your voicemail and check devices for malware when you return.

*Cyber criminals from numerous countries buy and sell stolen financial information including credit card data and login credentials (user names and passwords).*

### Reminder

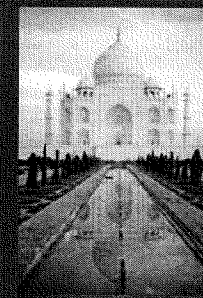
*Our country will be judged by the impression you make. As an American abroad, you serve as a spokesperson for the United States.*

Additional travel security tips and country threat assessments are available from the FBI upon request.

Your local FBI office #: \_\_\_\_\_

[www.fbi.gov](http://www.fbi.gov)

U.S. Department of Justice  
Federal Bureau of Investigation



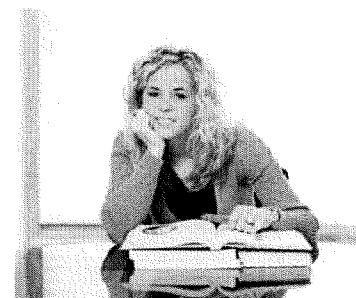
# SAFETY AND SECURITY for US Students Traveling Abroad

*Living and studying in another country will be an enriching and rewarding experience, especially if you are prepared and take certain precautions.*

*This brochure will introduce you to threats you may face and provide tips on avoiding unsafe situations. Following these precautions will reduce your risk of encountering problems.*

Did You Know?

Groups of children and teens may swarm you and forcibly steal your personal belongings.



**"Act Smart. Be Safe."**



An ounce of prevention is worth a pound of cure.



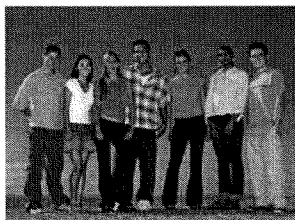
## Before You Go

Familiarize yourself with local laws and customs in the areas you plan to travel. You are expected to obey their laws, which may include dress standards, photography restrictions, telecommunication restrictions, curfews, etc.

### Plan your wardrobe

so that it does not offend the locals, nor draw unwanted attention to yourself.

Americans are perceived as wealthy and are targeted for pick pocketing and other crimes. Do not wear expensive-looking jewelry and avoid wearing American team sports shirts or baseball caps that might indicate you are an American.



**Make copies of your passport, airplane ticket, driver's license, and credit cards** that you take with you. Keep one copy at home; carry a second copy with you but separate from the originals. This will help speed the replacement process if they are lost or stolen.

## During Your Stay

**Protect your passport!** Theft of American tourist passports is on the rise. It is recommended that you carry your passport in a front pants pocket or in a pouch hidden in your clothes, and that it remain with you at all times. Some hotels require you to leave it at the desk during your stay and they may use it to register you with the local police—a routine policy. Ask for a receipt and be sure to retrieve your passport before continuing your trip. If your passport is lost or stolen, report the situation immediately to the nearest US Embassy or Consulate.



**Do not invite strangers into your room.**

**Be courteous and cooperative** when processing through customs. Do not leave your bags unattended. Stay alert.

**Do not take unnecessary identification or credit cards** in case they are stolen. Take only what is necessary. Obtain traveler's checks if needed.

**Establish points of contact** for your family to contact and for your foreign hosts to contact in the event of an emergency. Register your trip with the State Department.

**Take any necessary medications** with you in their original containers and keep them in your carry-on luggage (not checked baggage) during the flight. Verify you have adequate medical insurance.

**Obtain specific pre-travel country risk assessments** for the country/countries you plan to visit from your study abroad program manager, the State Department, and/or the FBI. There may be specific issues you should be aware of and prepare for that will ensure your safety and peace of mind.

### Useful websites:

State Department Students Abroad:

[www.studentsabroad.state.gov](http://www.studentsabroad.state.gov)

State Department travel website:

[www.state.gov/travel](http://www.state.gov/travel)

Center for Disease Control for Travelers' Health:

[www.cdc.gov](http://www.cdc.gov)

**Use only authorized taxis.** Passengers have been robbed or kidnapped when using "gypsy" taxis.

**Avoid traveling alone**, especially after dark. Be conscious of your surroundings and avoid areas you believe may put your personal safety at risk. Be wary of street vendors and innocent-looking youngsters. While one person has your attention, another may be picking your pocket.



**Do not carry large amounts of cash.** Always deal with reputable currency exchange officials or you run the risk of receiving counterfeit currency. Keep a record of your financial transactions.

**Beware that theft** from sleeping compartments on trains is common.

**Do not leave drinks unattended** – someone could slip a drug into it that causes amnesia and sleep.

**Avoid long waits in lobbies and terminals**, if possible. These areas may harbor pickpockets, thieves, and violent offenders. Laptop theft is especially common in airports.

***In an international airport, a thief positioned himself to walk in front of a traveler who was walking with his roll bag. The thief stopped abruptly in front of the traveler causing the traveler to also stop. A second thief was following and quickly removed the traveler's laptop from his roll bag and disappeared.***

**Avoid civil disturbances and obey local laws.** If you come upon a demonstration or rally, be careful; in the confusion you could be arrested or detained even though you are a bystander. Be mindful that in many countries, it is prohibited to speak derogatorily of the government and its leaders. It may be illegal to take photographs of train stations, government buildings, religious symbols, and military installations.

**Avoid actions that are illegal, improper or indiscreet.** Avoid offers of sexual companionship; they may lead to a room raid, photography, and blackmail. Do not attempt to keep up with your hosts in social drinking. Do not engage in black market activities. Do not sell your possessions. Do not bring in or purchase illegal drugs or pornography. Do not seek out political or religious dissidents. Do not accept packages or letters for delivery to another location.

***An American was given a letter by a man he had never met. He tried to return the letter but the man ran away. That evening, national security officers visited the American, admonished him for taking the letter, and required him to sign a statement concerning the event.***

If you are arrested for any reason, ask to notify the nearest US Embassy or Consulate. A consular officer cannot arrange for free legal aid or provide bail money, but they can assist you. Do not admit to wrongdoing or sign anything. Do not agree to help your detainer.

**Keep a low profile and shun publicity.** Do not discuss personal or family information with local

news media, and as a general rule, be careful what information you share with foreigners. They may have been directed to obtain information about you for duplicitous purposes and may use what they learn to target or use against you.

**Evade criminals and terrorists by being aware of your surroundings** and alert to the possibility of surveillance. Take mental notes of anyone following you and promptly report it to the appropriate security officials and/or the US Embassy or Consulate. In general, criminals will strike when their target seems most vulnerable and lax about his/her security. If anyone grabs you, make a scene-- yell, fight and try to get away! If you are kidnapped, remain alert and establish a program of mental and physical activity for yourself; try to remain calm and non-threatening.

***"Turkey drop" scam: a person drops money in front of a victim while an accomplice waits for the money to be picked up and suggests splitting it. The first person returns and accuses both of stealing the money. This usually results in the victim's money being stolen.***

**Beware of new acquaintances who probe for information** about you or who attempt to get you involved in what could become a compromising situation.

**Do not gossip about character flaws, financial problems, emotional relationships, or other difficulties** of your fellow Americans or yourself. This information is eagerly sought by those who want to exploit you or your fellow travelers.

**Beware that your conversations may not be private or secure.** Unlike the United States, most other countries do not have legal restrictions against technical surveillance. Most foreign security services have various means of screening incoming visitors to identify persons of potential intelligence interest. They also have well established contacts with hotels and common hosts that can assist in various forms of monitoring you.

***Two American students on study abroad talked privately about the lighting in their apartment. The next day, a light that had been out for weeks was working.***



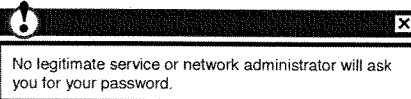
## Preventive Measures at Work:

- "Defense in Depth" – use multiple layers of security throughout the computer network.
- Identify ways you have lost data in the past and mitigate those threats. Educate employees about those threats and how to change their behavior, if necessary, to prevent future loss.
- Constantly monitor data movement on your network.
- Establish policies and procedures for intrusion detection systems on company networks.
- Establish policies about what company information can be shared on blogs or personal social web pages. Enforce the policy.
- Educate employees about how their own online behavior could impact the company.
- Provide yearly security training.
- Ask employees to report suspicious incidents as soon as possible.

## Additional Preventive Measures:

- Do not store any information you want to protect on any device that connects to the Internet.
- Always use high security settings on social networking sites, and be very limited in the personal information you share. Monitor what others are posting about you on their online discussions.
- Use anti-virus and firewall software. Keep them, your browser, and operating systems patched and updated.
- Change your passwords periodically, and do not reuse old passwords. Do not use the same password for more than one system or service. For example, if someone obtains the password for your email, can they access your online banking information with the same password?
- Do not post anything that might embarrass you later or that you don't want strangers to know.
- Verify those you correspond with. It is easy for people to fake identities over the Internet.
- Do not automatically download, or respond to content on a website or in an email. Do not click on links in email messages claiming to be from a social networking site. Instead go to the site directly to retrieve messages.
- Only install applications or software that come from trusted, well-known sites. "Free" software may come with malware. Verify what information applications will be able to access prior to enabling them. Once installed, keep it updated. If you no longer use it, delete it.

- Disable Global Positioning System (GPS) encoding. Many digital cameras encode the GPS location of a photo when it is taken. If that photo is uploaded to a site, so are the GPS coordinates, which will let people know that exact location.
- Whenever possible, encrypt communications with websites. It may be a feature social network sites allow you to enable.
- Avoid accessing your personal accounts from public computers or through public WiFi spots.
- Beware of unsolicited contacts from individuals in person, on the telephone, or on the Internet who are seeking corporate or personal data.
- Monitor your bank statements, balances, and credit reports.
- Do not share usernames, passwords, social security numbers, credit cards, bank information, salaries, computer network details, security clearances, home and office physical security and logistics, capabilities and limitations of work systems, or schedules and travel itineraries.



- Do not provide information about yourself that will allow others to answer your security questions—such as when using "I forgot my password" feature.
- Be thoughtful and limit personal information you share such as job titles, locations, hobbies, likes and dislikes, or names and details of family members, friends, and co-workers.

## Educational Resources:

A number of organizations and websites provide additional details on how to protect you and your workplace from Internet social networking threats.

[www.LooksTooGoodToBeTrue.com](http://www.LooksTooGoodToBeTrue.com)

[www.OnGuardOnline.gov](http://www.OnGuardOnline.gov)

[www.us-cert.gov](http://www.us-cert.gov)

[www.ic3.gov](http://www.ic3.gov)

[www.dhs.gov](http://www.dhs.gov)

[www.ftc.gov](http://www.ftc.gov)

[www.fbi.gov](http://www.fbi.gov)



U.S. Department of Justice  
Federal Bureau of Investigation

# INTERNET SOCIAL NETWORKING RISKS

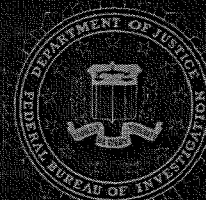
INTERNET-BASED SOCIAL NETWORKING SITES HAVE CREATED A REVOLUTION IN SOCIAL CONNECTIVITY. HOWEVER, CON ARTISTS, CRIMINALS, AND OTHER DISHONEST ACTORS ARE EXPLOITING THIS CAPABILITY FOR NEFARIOUS PURPOSES.

THERE ARE PRIMARILY TWO TACTICS USED TO EXPLOIT ONLINE SOCIAL NETWORKS.

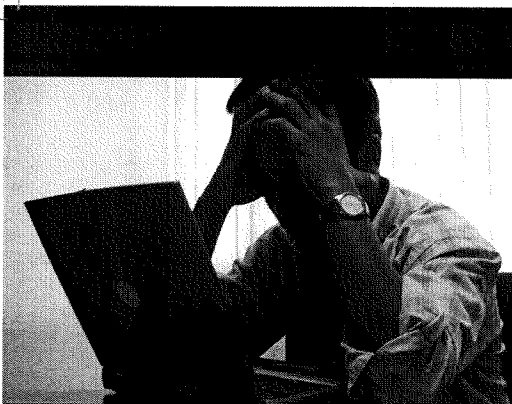
IN PRACTICE, THEY ARE OFTEN COMBINED.

**1. COMPUTER SAVVY HACKERS WHO SPECIALIZE IN WRITING AND MANIPULATING COMPUTER CODE TO GAIN ACCESS OR INSTALL UNWANTED SOFTWARE ON YOUR COMPUTER OR PHONE. 2. SOCIAL OR HUMAN HACKERS WHO SPECIALIZE IN EXPLOITING PERSONAL CONNECTIONS THROUGH SOCIAL NETWORKS. SOCIAL HACKERS, SOMETIMES REFERRED TO AS "SOCIAL ENGINEERS," MANIPULATE PEOPLE THROUGH SOCIAL INTERACTIONS (IN PERSON, OVER THE PHONE, OR IN WRITING).**

HUMANS ARE A WEAK LINK IN CYBER SECURITY, AND HACKERS AND SOCIAL MANIPULATORS KNOW THIS. THEY TRY TO TRICK PEOPLE INTO GETTING PAST SECURITY WALLS. THEY DESIGN THEIR ACTIONS TO APPEAR HARMLESS AND LEGITIMATE.







Falling for an online scam or computer hack could be damaging for an individual victim as well as the organization the victim works for. Such risks include:

- Identity theft / Impersonation
- Harassment
- Peer pressure
- Loss of employment
- Damaged business reputation
- Damaged career or personal reputation
- Damaged data or networks
- Intellectual property theft / Data theft
- Brand hijacking
- Delays or interruption in production
- Lost revenue or income
- Burglary
- Target for spam and phishing
- Content alteration of websites
- Malware and virus dissemination

There are many tactics people may use to trick others into providing information or granting access to that information through social networking venues. Although not exhaustive, this brochure lists some of these tactics and suggests ways to mitigate online social networking risks.

#### EXAMPLE

You receive a message from a friend on your social networking site. The message directs you to view a video on another site. When you go to that site, a message pops up and says you need to download a newer version of software. However, the software update is really malware that, when downloaded, gives control of your computer to the creators of the malware. (In some cases, simply visiting the site will download the malware.) The malware then sends a message to all your "friends" on your social networking site directing them to the same site with the malware. The malware creators soon have multiple computers under their control (a "botnet").

## Vulnerability of Social Networking Sites

Social networking sites are Internet-based services that allow people to communicate and share information with a group.

### Risks:

Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you may become. Even when using high security settings, friends or websites may inadvertently leak your information.

Personal information you share could be used to conduct attacks against you or your associates. The more information shared, the more likely someone could impersonate you and trick one of your friends into sharing personal information, downloading malware, or providing access to restricted sites.

Predators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation.

Information gleaned from social networking sites may be used to design a specific attack that does not come by way of the social networking site.

### Tactics:

**Baiting** - Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer.

Do not use any electronic storage device unless you know its origin is legitimate and safe. Scan all electronic media for viruses before use.

**Click-jacking** - Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking scams have employed "Like" and "Share" buttons on social networking sites.

Disable scripting and iframes in whatever Internet browser you use. Research other ways to set your browser options to maximize security.

**Cross-Site Scripting (XSS)** - Malicious code is injected into a benign or trusted website. A Stored XSS Attack is when malicious code is permanently stored on a server; a computer is compromised when requesting the stored data. A Reflected XSS Attack is when a person is tricked into clicking on a malicious link; the injected code travels to the server then reflects the attack back to the victim's browser. The computer deems the code is from a "trusted" source.

Turn off "HTTP TRACE" support on all web servers. Research additional ways to prevent becoming a victim of XSS.

**Doxing** - Publicly releasing a person's identifying information including full name, date of birth, address, and pictures typically retrieved from social networking site profiles.

Be careful what information you share about yourself, family, and friends (online, in print, and in person).

**Elicitation** - The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated.

Be aware of elicitation tactics and the way social engineers try to obtain personal information.

**Pharming** - Redirecting users from legitimate websites to fraudulent ones for the purpose of extracting confidential data. (E.g.: mimicking bank websites.)

Watch out for website URLs that use variations in spelling or domain names, or use ".com" instead of ".gov", for example. Type a website's address rather than clicking on a link.

#### EXAMPLE

Most computer infections come from websites. Just visiting a website can expose your computer to malware even if you do not download a file or program. Often legitimate sites may be unknowingly infected.

Websites with information on popular celebrities or current sensational news items are frequently hijacked by criminals, or criminals may create such websites to lure victims to them.

**Phishing** - Usually an email that looks like it is from a legitimate organization or person, but is not and contains a link or file with malware. Phishing attacks typically try to snag any random victim. Spear phishing attacks target a specific person or organization as their intended victim.

Do not open email or email attachments or click on links sent from people you do not know. If you receive a suspicious email from someone you know, ask them about it before opening it.

#### EXAMPLE

In March 2011, hackers sent two spear phishing emails to a small group of employees at security firm, RSA. They only needed one employee to open an infected file and launch the malware. The malware downloaded information from RSA that then helped the hackers learn how to defeat RSA's security token. In May and June 2011, a number of defense contractors' networks were breached via the compromised RSA token.

**Phreaking** - Gaining unauthorized access to telecommunication systems.

Do not provide secure phone numbers that provide direct access to a Private Branch Exchange or through the Public Branch Exchange to the public phone network.

**Scams** - Fake deals that trick people into providing money, information, or service in exchange for the deal.

If it sounds too good to be true, it is most likely a scam. Cybercriminals use popular events and news stories as bait for people to open infected email, visit infected websites, or donate money to bogus charities.

#### EXAMPLE

Before the 2010 World Cup, cybercriminals offered tickets for sale or sent phishing emails claiming you won tickets to see the event.

After the death of Osama Bin Laden, a video claiming to show Bin Laden's capture was posted on Facebook. The video was a fake. When users clicked on the link to the video, they were told to copy a JavaScript code into their browser bar which automatically sent the hoax to their friends, and gave the hackers full access to their account.

**Spoofing** - Deceiving computers or computer users by hiding or faking one's identity. Email spoofing utilizes a sham email address or simulates a genuine email address. IP spoofing hides or masks a computer's IP address.

Know your co-workers and clients and beware of those who impersonate a staff member or service provider to gain company or personal information.



April 2011

# Higher Education and National Security:

## The Targeting of Sensitive, Proprietary and Classified Information on Campuses of Higher Education



This white paper was prepared by the Counterintelligence Strategic Partnership Unit of the FBI.  
This paper is unclassified in its entirety.



## Foreword

This white paper was prepared by the FBI's Counterintelligence Strategic Partnership Unit to provide awareness to administrators, senior researchers, export control offices, and technology transfer offices at higher education institutions about how foreign intelligence services and non-state actors use US colleges and universities to further their intelligence and operational needs. This paper is unclassified and fulfills part of the FBI's goal of building awareness with public and private entities about counterintelligence risks and national security issues.

## Executive Summary

The United States is a society of openness and freedom, values especially central to campuses of higher education. Foreign adversaries and competitors take advantage of that openness and have been doing so for many years.

There are foreign nations that seek to improve their economies and militaries by stealing intellectual property from a world technology leader like the United States. There are also foreign adversaries that seek to gain advantages over the United States. These nations use varied means to acquire information and technology to gain political, military, and economic advantages. There are also foreign companies and entrepreneurs who want to obtain research data in order to improve their own products or get to market first with innovative ideas or products being developed at US universities.

The open environment of US campuses of higher education may be misused in order to:

- Steal technical information or products
- Bypass expensive research and development
- Recruit individuals for espionage
- Exploit the student visa program for improper purposes
- Spread false information for political or other reasons

To accomplish one or more of the above goals, duplicitous or opportunistic actors or organizations may use a variety of methods such as:

- Conduct computer intrusions
- Collect sensitive research
- Utilize students or visiting professors to collect information
- Spot and recruit students or professors
- Send unsolicited email or invitations
- Send spies for language and cultural training, and to establish credentials
- Fund or establish programs at a university

Most foreign students, researchers, or professors studying or working in the United States are here for legitimate and proper reasons. Only a very small percentage is actively working at the behest of another government or organization. However, some foreign governments also pressure legitimate students to report information to intelligence officials, often using the promise of favors or threats to family members back home.



# Higher Education and National Security

## Introduction

American higher education institutions are centers of knowledge, discovery and intellectual exploration. The people of the United States value and take pride in the openness and opportunities for learning; they welcome foreign students and understand why other countries encourage and sponsor their own citizens to enroll in US universities. The knowledge, culture, and skills brought by foreign students enhance the educational experiences of other students and teachers. Due to globalization, today's college education is international in nature. Professors share their knowledge with students and colleagues—not just at their own university, but all over the world—and students from a variety of countries study together in the same program. Information is a valuable asset on campuses, and most of it is shared liberally; however, some information is private or restricted. Information that is not openly shared may include pre-publication research results, proprietary information, classified research, or certain lab techniques and processes.

## Who tries to improperly obtain information from US campuses?

There are a variety of people and organizations within and outside the United States who may seek to improperly or illegally obtain information from US institutions of higher education: foreign and domestic businesses, individual entrepreneurs, competing academics, terrorist organizations, and foreign intelligence services.

Foreign and domestic businesses compete in a global economy. Some foreign governments provide resources and information, including competitive intelligence gathering and corporate espionage on behalf of their indigenous companies as a way to promote the overall economic well-being of their country. Foreign intelligence services pursue restricted information and so may seek out people who have, or will eventually have, access to restricted information. Individual entrepreneurs may capitalize on opportunities to bring new technology or services to their country in order to fill a niche currently supplied by non-native companies. To jump start business, they may steal research or products that would otherwise be costly to create or replicate. Academics may steal research and use it or claim it as their own for a variety of reasons. Terrorist organizations may want information on products or processes they can use to inflict mass casualties or damage.

## What is a foreign intelligence service?

A foreign intelligence service is a foreign organization, usually part of the government, whose primary purpose is to gather and analyze information it deems valuable. Their ultimate goal for collecting information is to benefit their own country politically, militarily, and economically. Often the organization directs its agents to collect specific information on specific topics. An employee of an intelligence service who has been specially trained on how to collect and analyze information is an *intelligence officer*. The collected information or its analytic



product is *intelligence*. Another purpose of a foreign intelligence service is to spread the influence and ideology of its regime, or damage the claims and image of another regime. In this case, the intelligence service *provides* information. This may be done openly through propaganda, diplomatic statements, offers of training, or covertly using rumor, false-news stories, fabricated studies, bribery, or any number of other means.

Foreign intelligence services target information. To get to the information they will target people who have that information or who might be able to get the information in the future—someone with placement and access. The open environment of a university is an ideal place to find recruits, propose and nurture ideas, learn, and even steal research data, or place trainees who need to be exposed to our language and culture—a sort of on-the-job-training for future intelligence officers. Foreign intelligence services have been taking advantage of higher education institutions and personnel for many years, either through deliberate stratagems or by capitalizing on information obtained through other parties. Intelligence services are patient, sometimes waiting several years before expecting a return on an intelligence investment. Foreign intelligence services, by their nature, are secretive and unobtrusive. A successful operation by a foreign intelligence service is one where a target never knows they interacted with that service.

### **Why target university campuses?**

#### *To Obtain Restricted Information or Products*

Despite university warnings on the restrictions on his research, University of Tennessee professor Reece Roth employed a Chinese and an Iranian student to assist in plasma research while working on a classified US Air Force project that stipulated no foreign nationals could work on the project. Roth also traveled to China with his laptop computer containing export-restricted information and had a sensitive research paper emailed to him there through a Chinese professor's email account. Roth claimed the research was "fundamental" and not sensitive, but a jury concluded otherwise.<sup>1</sup> In September 2008, Roth was found guilty on 18 counts of conspiracy, fraud, and violating the Arms Export Control Act; he was later sentenced to four years in prison.<sup>a</sup>

A country or company does not have to orchestrate the actual theft of the research in order to capitalize on it. It is unknown how the Chinese used the information they obtained from Roth, but because they invited him to visit China and he had a sensitive report emailed to him while there, it should be assumed they were interested in his research and planned to utilize it.

The US government has determined some technologies should not be shared with other countries because it would remove that technological edge that serves to protect the United States (militarily, economically, or otherwise), or the technology would be dangerous in the hands of certain groups. The knowledge of how to counter US technological advantages is also protected. Organizations that research, test, or

#### **Export restrictions of goods and technology**

- US Department of Commerce Export Administration Regulations (EAR) - "Dual Use" items
- US Department of State International Traffic in Arms Regulations (ITAR) - Inherently "Military Use" items
- US Department of Treasury Office of Foreign Assets Control (OFAC) - Trade Embargoes

<sup>a</sup> Atmospheric Glow Technologies, the company set up to commercialize plasma research and the lab where the US Air Force project was researched, pled guilty to 10 counts of exporting defense-related materials.



manufacture restricted technologies may be enjoined from exporting them to other countries without first obtaining approval. Providing export-restricted items or information to a foreign national located in the United States may be regarded, under export control law, as equivalent to exporting the item or information because it is now in the actual possession of a foreign national.

### *To Bypass Expensive Research & Development*

Sergei Tretyakov was the head of political intelligence for Russia's foreign intelligence service, the SVR,<sup>b</sup> in New York City from 1995-2000. In other words, he was a Russian spy. He described how a man in California traveled to New York, met with an SVR agent, and handed over years of US government funded medical research. The research studies had not been released to the public because many of them contained proprietary information based on medical patents held by US companies. The man who provided the data to the SVR agent was a Russian immigrant who wanted to help Russia and refused to be paid for the information; however, he did agree to be reimbursed for his air travel. Tretyakov observed:

The reports were extremely technical, and I noticed each had a dollar amount in the index that described exactly how much the US government had spent to pay for this research....[Russia obtained] scientific research that cost the US government forty million dollars for the price of eight hundred dollars in airplane tickets!<sup>2</sup>

As this case shows, a country or private company can save much time and money by bypassing research and development and jumping directly to an applied or practical application. Again, the organization does not have to direct someone to steal information in order to benefit from its theft. When a foreign company uses stolen data to produce products, at a reduced cost, that compete against American products, this can have direct harmful consequences for US businesses, and for universities that might receive revenue through patents and technology transfer.

While information is shared on campuses, there is still an ethical, and sometimes legal, responsibility to protect research. With the extensive amount of primary research done at universities, many researchers hope to gain recognition for innovative research. However, if their research is published by someone else first, they may lose that distinction and credit. Research is often funded by private companies or the government who may need a first-to-market practical application from the research to make it worth their investment. Stealing the research then could equate to stealing money from the funding organization.

### *To Find Recruits to Place in Valuable Positions*

Ana Montes agreed to assist the Cuban Intelligence Service while she was a graduate student pursuing a master's degree in International Studies from Johns Hopkins University. Upon graduation, she specifically sought and obtained employment where she could acquire information valuable to Cuba. She worked as a Latin America analyst at the Defense Intelligence Agency and provided classified information to Cuba on a regular basis for sixteen years until she was arrested in 2001. Perhaps the worst damage of her spying was that Cuba shared the information she provided with other countries not friendly to the United States. It is

---

<sup>b</sup> The *Sluzhba Vneshney Razvedki*, or SVR, is one component of the old Soviet KGB service.



also likely her information contributed to the death and injury of American and pro-American forces in Latin America.<sup>3</sup> Not only did Montes provide information to the Cubans, but she shaped analysis and thereby influenced US policy toward Latin America. After her arrest, Montes claimed she spied for Cuba because she did not agree with US policy toward Cuba and Nicaragua in the 1980s. It is believed she voiced this opinion during graduate school, and someone alerted the Cuban Intelligence Service and recommended her as a potential recruit. She did not expect to be paid by the Cubans for her service and received very little remuneration from them. She is now serving 25 years in prison.

Ana Montes is an example of a spy motivated by ideology. US college campuses are an especially good place to look for people with particular ideological views. Campuses are known for their open discussions and debates. Foreign intelligence services sometimes find students with particular political or ideological beliefs by attending campus rallies, by interacting with particular clubs, or reading campus newspapers and blogs. When they discover someone they think will help, they may approach that person and entice him/her to join their cause.

Cuba has sought other ideological recruits. Kendall Myers worked as an adjunct professor at Johns Hopkins University School of Advanced International Studies and as a contract instructor at the State Department's Foreign Service Institute. Intrigued by Cuba, he accepted an invitation to visit. The Cubans assessed Myers as one who would help Cuba, and recruited him as a spy. They encouraged Myers to get a job with the State Department or the CIA. Myers returned to being an instructor with the State Department in 1980, and eventually worked full-time in the State Department's Bureau of Intelligence and Research until he retired in 2007. Myers took classified information and, with the help of his wife, passed it to Cuba. He and his wife were arrested in June 2009 and pled guilty to serving as illegal agents of Cuba for nearly thirty years. Myers was sentenced to life in prison and his wife was sentenced to 81 months.<sup>4</sup>

While it is not a crime in the United States to hold particular political or ideological ideals, it is a crime to pass classified information to those not authorized to receive it. Both Montes and Myers specifically sought positions within US government agencies that gave them greater access to classified information with the goal of passing that information to a foreign nation.

Foreign intelligence services use a variety of enticements to recruit spies: money, blackmail, revenge, and flattery, for example.

#### *To Exploit the Student Visa Program for Improper Purposes*

Khalid Ali-M Aldawsari, a Saudi student studying chemical engineering at Texas Tech University, was arrested in February 2011 on a charge of attempted use of a weapon of mass destruction. A notebook was found at Aldawsari's residence that appeared to be a diary or journal:

[E]xcerpts indicate that Aldawsari had been planning to commit a terrorist attack in the United States for years. One entry describes how Aldawsari sought and obtained a particular scholarship because it allowed him to come directly to the United States and helped him financially, which he said "will help tremendously in providing me with the support I need for Jihad."<sup>5</sup>



### *To Spread False Information for Political or Other Reasons*

According to Sergei Tretyakov, a former KGB/SVR officer, the KGB ordered the Soviet Academy of Sciences to come up with a report that would scare the Western public and keep NATO from placing Pershing missiles in Western Europe:

The story, which had been approved by KGB propagandists, described experiments in the Karakum desert in South Central Asia that were being done by a Soviet specialist in atmospheric physics... [Other Soviet] scientists claimed they had used a mathematical model to estimate how much dirt and debris would be blasted into the atmosphere during a nuclear attack in Germany.<sup>6</sup>

The KGB had the report published in a Swedish journal. In the intelligence world, this is called disinformation. Disinformation may be blatant deception or small fabricated kernels in a large milieu of reliable facts. In the academic arena where research is often based on previous research, when results from a study can be shared quickly and easily with other researchers, it is important to science that people share *accurate* results. If subsequent research is based on incorrect data, many of those subsequent conclusions could be inaccurate as well. Expanding scientific horizons is not always the main motivating factors for research or publications in other countries. Foreign researchers may be under pressure to make their research conclude what their government wants it to conclude, or they may be ordered to write completely fabricated studies.

### **What methods are used to target information at US universities?**

#### *Conduct Computer Intrusions*

Today's computer-connected world provides abundant access for criminals, terrorists, opportunists, and intelligence services to exploit the access cyber networks afford. They can hack into a system and steal research and other information, send phishing email with malware attached, and exploit social networking sites. They search for restricted information, people who have access to the information, and information that can be used to coerce or entice people with access to share restricted data. There have been computer intrusions into US universities from numerous countries. US universities receive large numbers of unsolicited requests for information and millions of hits on their Web servers each day. Computer hackers, especially those funded by a foreign government, are capable of breaching firewalls and exploiting vulnerabilities in software. They are also skilled at deceiving trusting or unassuming individuals through scams.

#### *Collect Sensitive Research*

A possible scenario: An Asian student gets accepted into a graduate program at a US university. The student has connections with a research group at a university back in Asia and is allowed to establish a formal collaboration between the two research labs. The Asian student invites personnel from the Asian university lab to visit the US university. Without permission, the visitors take photographs of all the equipment in the lab including the make and model of the equipment in order to reproduce the US university's lab at the Asian university. About a year into the collaboration, the graduate advisor becomes concerned that too much information is



going out to the Asian research lab and not enough is coming back to the US university. Although the research is unrestricted, the graduate advisor recognizes that applications of the research could have national security implications. The Asian lab has more resources and is able to follow-up on ideas more quickly but the sharing of data and results is unbalanced, so the graduate advisor decides to end the collaboration.

Sometimes, as research develops, the application of that knowledge leads to products that have national security implications. Defectors and double-agent operations have affirmed intelligence services are very interested in acquiring technologies during the research and development phase regardless of classification,<sup>7</sup> since the application and new research may later become classified.

#### *Utilize Students or Visiting Professors to Collect Information*

Andrey Bezrukov was arrested in June 2010 for being an agent of Russia. He was a spy who entered the United States under an assumed name (Donald Heathfield) and false past. He attended Harvard's Kennedy School of Government from 1999-2000 and earned a Masters in Public Administration. After graduating, Bezrukov developed associations with professors at various universities including George Washington University and Oxford University. He allegedly targeted a professor who was once Al Gore's national security advisor. Bezrukov also attended Kennedy School reunions, specific society meetings, and think tank events that gave him access and exposure to people as he socialized with policy-makers and tried to cultivate intelligence targets.<sup>8</sup>

In this case, Russia sent a spy to a US university in order for him to cultivate friendships and associations with students and professors likely to move on to government positions. He therefore had a seemingly innocent basis to get off-the-record and inside information from any "friend" in a position with access to information.

Some countries may recruit students before they come to the United States and task them to send technological information they acquire back to their home country. Students may comply based upon a sense of loyalty for their home country's government or as a result of coercion and exploitation. In some instances, foreign students are funded by their government and therefore can serve, at no cost to the US university, as assistants to professors doing research in a targeted field, which gives the student access to the research data and its applications. Some countries may direct the student to seek US citizenship giving them greater access to restricted research. Most information taught at universities is available to anyone who enrolls. However, when information is classified, patented, proprietary, or export restricted, there are rules and laws imposed to protect and control that information.

Foreign business competitors may also send employees as students in order to obtain information valuable to their company. They may misrepresent themselves as students and not acknowledge their employment with a foreign company. A possible scenario: In order to obtain competitive intelligence or insider information on Business A, Business B has one of their employees apply and enroll in a program at a university that is doing research for and funded by their competitor, Business A. That employee/student may even apply for an internship at Business A. The unsuspecting Business A would not imagine a student intern was already a full employee of their competitor.



### *Spot Students or Professors with Access*

In 2009, Russia sent the following instructions to one of its spies, Lidiya Gurveva (using the name Cynthia Murphy), while she was pursuing an MBA degree at Columbia Business School, Columbia University:

[S]trengthen...ties w. classmates on daily basis incl. professors who can help in job search and who will have (or already have) access to secret info... [r]eport to C[enter] on their detailed personal data and character traits w. preliminary conclusions about their potential (vulnerability) to be recruited by Service.<sup>9</sup>

They also directed her to “ ‘dig up’ personal data of those students who apply (or are hired already) for a job at CIA.”<sup>10</sup> Guryeva was arrested in June 2010 for acting as an agent of a foreign power and was deported back to Russia.

This example demonstrates a foreign intelligence service searching for students who may soon have access to targeted information. Intelligence services also collect information on the programs, officers, professors, and demographics of US universities. After studying the information and, if they find a person to target, they will study his/her motivations, weaknesses, politics, and ambitions. Familiarizing themselves with a professor's work will help them determine a pretext for contacting the professor and how best to influence or recruit the professor.<sup>11</sup> They may spend years targeting an individual, and develop a relationship whereby the student or professor provides information, either wittingly or unwittingly, to the foreign country. For example, the foreign intelligence service may capitalize on existing political or social biases whereby they can coax a professor to share information based on a real or perceived cause (e.g. Myers). They may appeal to the ethnic nationality of a student and ask him/her to help their ancestral homeland. They may invite a professor to visit their country (e.g. Roth), sometimes at no expense to the professor. While the professor is in country, the government may gain access to the professor's digital storage devices (laptop, PDA, cell phone) and obtain sensitive research and personal information. The foreign intelligence service may use information to coerce or entice the professor to provide data in the future. Likewise, American students on study abroad may be evaluated as potential recruits by the host country's intelligence service.

Foreign agents often target students or professors from their own country first, anticipating they will agree out of a sense of patriotism or nationalism. However, they will also target anyone who appears to have the potential to be a good recruit.

### *Send Spies for Language and Cultural Training and to Establish Credentials*

As discussed above with Bezrukov and Guryeva, some foreign students are not here in order to obtain a traditional university education. They attend college in the United States to increase their understanding of the language and culture, make contacts, gain an education in a particular field, and send information back to their home country. In some cases, they may lay low and do nothing criminal for several years.

Li Fengzhi was a Chinese intelligence agent for thirteen years before the Chinese Ministry of State Security sent him to the United States, in 2003, to pursue a doctoral degree in international politics and diplomatic philosophy at the University of Denver. Shortly after his



arrival, Li requested and was granted political asylum in the United States.<sup>12</sup> While he has not disclosed why the Chinese sent him to come to the United States as a graduate student, it is plausible the Chinese thought a student cover would make him more innocuous and able to collect information and make personal connections, or provide him with exposure and experience.

#### *Send Unsolicited Email or Invitations*

A foreign intelligence agent, business competitor, or other duplicitous actors may pose as a researcher and send an unsolicited email to a US researcher in the hopes of establishing contact or getting answers to a question. They may send unsolicited invitations to submit papers or attend conferences. They may use flattery or seek information that can be further used to target the researcher or someone with better access. Sometimes the unsolicited email is a request to review someone else's research or technology paper. In this case, the duplicitous actor is hoping the targeted professor will correct mistakes he/she sees in the provided paper and, in that way, obtain valuable insights and restricted information. Unlike computer intrusions, unsolicited email may not have attached malware but is an attempt to start a correspondence. It is a quick and cheap way to test whether a targeted person will respond and, if so, what subject will cause them to respond. If information can be obtained via simple email exchange, it will save time, effort, and money.

A possible scenario: A researcher at a US university receives an email asking to collaborate. He does not recognize the sender, but would like to collaborate and decides to respond. The sender asks for data on how to conduct a particular experiment, and the US researcher responds hoping to get the results of the experiment. The sender of the email provides a draft paper and asks for input; the US professor notes errors in the paper and corrects them. In the meantime, the sender asks for more data or research clarifications. Several months later, the US researcher realizes that for all the "collaboration" the two have been doing, he has no idea of the true identity or location of the sender, has received no information of value in return, and it now appears the sender was essentially milking the US researcher for unpublished and sensitive information.

Another possible scenario: A researcher receives an unsolicited invitation to submit a paper for an international conference. She submits a paper and it is accepted. At the conference, the hosts ask for a copy of her presentation. The hosts hook a thumb drive to her laptop, and unbeknownst to her, download every file and data source from her computer.

#### *Fund or Establish Programs at a University*

In 2005 Belgium's intelligence agency, Sûreté de l'Etat, announced the defection of a Chinese spy who had been coordinating industrial espionage agents throughout Europe for ten years. During that time, the defector worked at European universities and was a member of the Chinese Students and Scholars' Association of Leuven. "According to an intelligence official, the association enabled Beijing's Ministry of State Security to maintain contact with a wide spectrum of Chinese citizens living across the continent."<sup>13</sup> The defector gave the Sûreté de l'Etat the names and activities of hundreds of people who were supplying information to China from a variety of business organizations.



It is easier for a spy to operate in an environment where he is trusted than where he is scrutinized. An organization may donate money or goods to a university to establish cultural centers, fund academic programs, or facilitate joint research. The funding agency may place stipulations on how the programs or centers are run—stipulations that ultimately benefit that organization. The funding organization may be able to place their own recruits in positions with little or no oversight from the university. Donations also establish a good will attitude and build a sense of trust between the donating institution and the university.

### **How many foreign students are in the United States for duplicitous reasons?**

Most foreign students, researchers, or professors studying or working at US universities are here for legitimate and proper reasons. Based on interviews, observations, defector information, and double-agent operations, the FBI concludes that only a small percentage of foreign students or visiting professors are actively working at the behest of their government or other organizations.

### **Why is the FBI concerned?**

The FBI is mandated to protect the nation from internal and external threats. National security priorities include:

- Keep Weapons of Mass Destruction (WMD) from falling into the wrong hands
- Protect the secrets of US Government agencies and US contractors
- Protect US critical assets

Beyond these goals, there are laws and regulations that seek to safeguard intellectual property, protect personal information, and ensure that government funding is used appropriately. These laws help protect US businesses, universities, and individuals from theft and fraud. Ultimately, it is every university's responsibility to safeguard their information. The FBI is actively partnering with universities to assist in those efforts. The FBI can provide counterintelligence tools and awareness training that will aid in recognizing what is suspicious behavior and how to better protect facilities and information. If invited, the FBI will collaborate with a US university or college on a broad array of areas relating to:

- Cyber security
- The safety and integrity of higher education in the United States
- Intellectual property developed through US university research
- Sensitive and classified research
- Researchers' ability to get first-to-market with their ideas
- Research funded by the US Government—ultimately by the US taxpayers
- Keeping US students and professors from being recruited by foreign intelligence services
- Personal and sensitive information (identity theft, fraud, stolen research, and so forth)
- Campus safety and safety awareness of US students studying abroad
- Animal rights terrorism
- Eco rights terrorism



### *National Security Higher Education Advisory Board*

The US Government created the National Security Higher Education Advisory Board (NSHEAB) in September 2005. It was designed to bridge historical gaps between the US Intelligence Community and academe with respect to national security issues and is comprised of approximately 20 presidents and chancellors who represent higher education institutions. The NSHEAB promotes cooperation and understanding between higher education and several government agencies to include the FBI.

### **Conclusion**

Knowledge and information are valuable assets and are an integral part of university activities, but not all campus information is for public consumption. Individuals and organizations that want to obtain innovative or restricted information may have ulterior motives and may misrepresent themselves and their intentions in order to gain access to restricted information, or they may outright steal it. This white paper provides a sampling of means used by duplicitous actors and organizations. Universities and researchers should protect their intellectual property and be cognizant that there are dishonest actors and organizations that take advantage of the environment of sharing on US campuses of higher education.



---

## Endnotes

<sup>1</sup> Associated Press, "Ex-Prof Gets 4 Years for Passing Military Secrets." 1 July 2009.

<sup>2</sup> Pete Earley, *Comrade J: The Untold Secrets of Russia's Master Spy in America after the End of the Cold War* (New York: G.P. Putnam's Sons, 2007), 274.

<sup>3</sup> Scott W. Carmichael, *True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy* (Annapolis MD: Naval Institute Press, 2007).

<sup>4</sup> Ginger Thompson, "Couple's Capital Ties Said to Veil Spying for Cuba." *New York Times* 19 June 2009. And United States Department of Justice. Press Release, "Former State Department Official and Wife Arrested for Serving as Illegal Agents of Cuba for Nearly 30 Years," 5 June 2009. And United States Department of Justice. Press Release, "Former State Department Official Sentenced to Life in Prison for Nearly 30-Year Espionage Conspiracy." 16 July 2010.

<sup>5</sup> United States Department of Justice Press Release, *Texas Resident Arrested on Charge of Attempted Use of Weapon of Mass Destruction*. 24 February 2011.

<sup>6</sup> *Comrade J*, 170-171.

<sup>7</sup> Bill Gertz, *Enemies: How America's Foes Steal Our Vital Secrets—and How We Let it Happen*. (New York: Crown Forum, 2006), 138.

<sup>8</sup> Evan Perez, "Alleged Russian Agent Claimed Official Was His Firm's Adviser." *The Wall Street Journal* 2 July 2010. And Naveen N. Srivatsa and Xi Yu. "Alleged Russian Spy Blends Into Harvard." *The Harvard Crimson* 30 June 2010.

<sup>9</sup> United States Department of Justice Affidavit, "US v Christopher R. Mestos et al," 1 June 2010.

<sup>10</sup> Ibid.

<sup>11</sup> Jose Cohen, "Castro's Intelligence Service and the US Academic Community." *ICCAS Monograph Series* January 2002.

<sup>12</sup> Jeff Stein, "Li Fengzhi, Ex-Chinese Spy, Granted Asylum." *The Washington Post* 5 October 2010. And Jeff Stein, "Li Fengzhi, Chinese Spy Who Defected to U.S., Facing Deportation." *The Washington Post* 2 September 2010.

<sup>13</sup> Damien McElroy, "China Aims Spy Network at Trade Secrets in Europe." *The Telegraph* 3 July 2005.





# The School Shooter: A Quick Reference Guide

BAU-1 (703) 632-4333



## REMEMBER

- There is not a "profile" of a school shooter- instead the students who carried out the attacks differed from one another in numerous ways.
- School shootings are rarely impulsive acts.
- They are typically thought out and planned in advance.
- Prior to most school shootings other students knew the shooting was going to occur but failed to notify an adult.
- Very few of the attackers ever directed threats to their targets before the attack.
- The most common goal was retribution. The justifications and excuses offered indicated this stemmed not from an absence of values but from a well-developed value system in which violence was acceptable.
- In many cases, other students were involved in the attack in some capacity.
- Many offenders experienced a significant personal loss in the months leading up to the attack, such as a death, breakup, or divorce in the family.
- Many offenders engaged in repetitive viewing of violent media and were often fascinated with previous school shootings. Repeated viewing of movies depicting school shootings, such as "Zero Day" and "Elephant," may indicate a fascination with campus attacks.
- Be aware of the subject's online videos, blogs, and social networking activities.

## Assessing Threatening Communications - Five Dimensions (Mohandie, 2000)

- Organized vs. disorganized thought processes
- Fixed vs. variable themes
- Focused vs. general target identification
- Violent action imperative vs. alternative coping means
- Short time imperative vs. lack of urgency

## Threat assessment - 11 Key Questions (U.S. Secret Service, 2002)

- What are the student's motive(s) and goals?
- Have there been any communications suggesting ideas or intent to attack?
- Has the student shown inappropriate interest in school attacks, weapons, and/or mass violence?
- Has the student engaged in any attack-related behaviors?
- Does the student have the capacity to carry out an act of targeted violence?
- Is the student experiencing hopelessness, desperation and/or despair?
- Does the student have a trusting relationship with at least one responsible adult?
- Does the student see violence as an acceptable/desirable way to solve problems?
- Is the student's version of events consistent with his/her actions?
- Are other people concerned about the student's potential for violence?
- What circumstances might affect the likelihood of an attack?

## Motives

- 24% motivated by desire for attention or recognition.
- 27% motivated by suicide or desperation.
- 34% motivated by attempt to solve a problem.
- 54% had multiple motives.
- 61% motivated by desire for revenge.
- 75% felt bullied/persecuted/threatened by others.

## Statistics

- 27% of attackers exhibited interest in violent movies.
- 37% of attackers exhibited interest in violence in their own writings, poems, essays, and journal entries.
- 59% of attacks occurred during the school day.
- 63% of attackers had a known history of weapons use.
- 68% acquired the weapon used from their own home or that of a relative.
- 93% of attackers engaged in some behavior prior to the attack that caused others to be concerned.
- 93% of attackers planned out the attack in advance.
- 95% of attackers were current students.
- Odds are one in 1 million that a student will die at school as a result of a violent act.

## Warning Signs

- Investigators should probe to discover if the subject has engaged in research, planning, or preparation (e.g., researched weapons or made attempts to obtain a weapon). Movement from thought to action represents a severe escalation of the risk of violence.
- In around 80% of school shootings at least one person had information that the attacker was thinking about or planning the school attack. In nearly 2/3, more than one person had information about the attack before it occurred. In nearly all of these cases, the person who knew was a peer, a friend, schoolmate, or sibling.
- Despite prompt law enforcement responses, most attacks were stopped by means other than law enforcement intervention.
- Be conscious of the "Werther Effect", defined as a duplication or copycat of another suicidal act. School shootings are typically well-publicized, sensationalized events that can trigger an increase in similar acts for roughly days or weeks after the attack.

## Resources

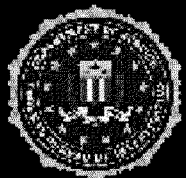
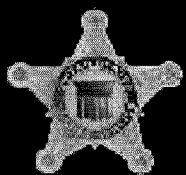
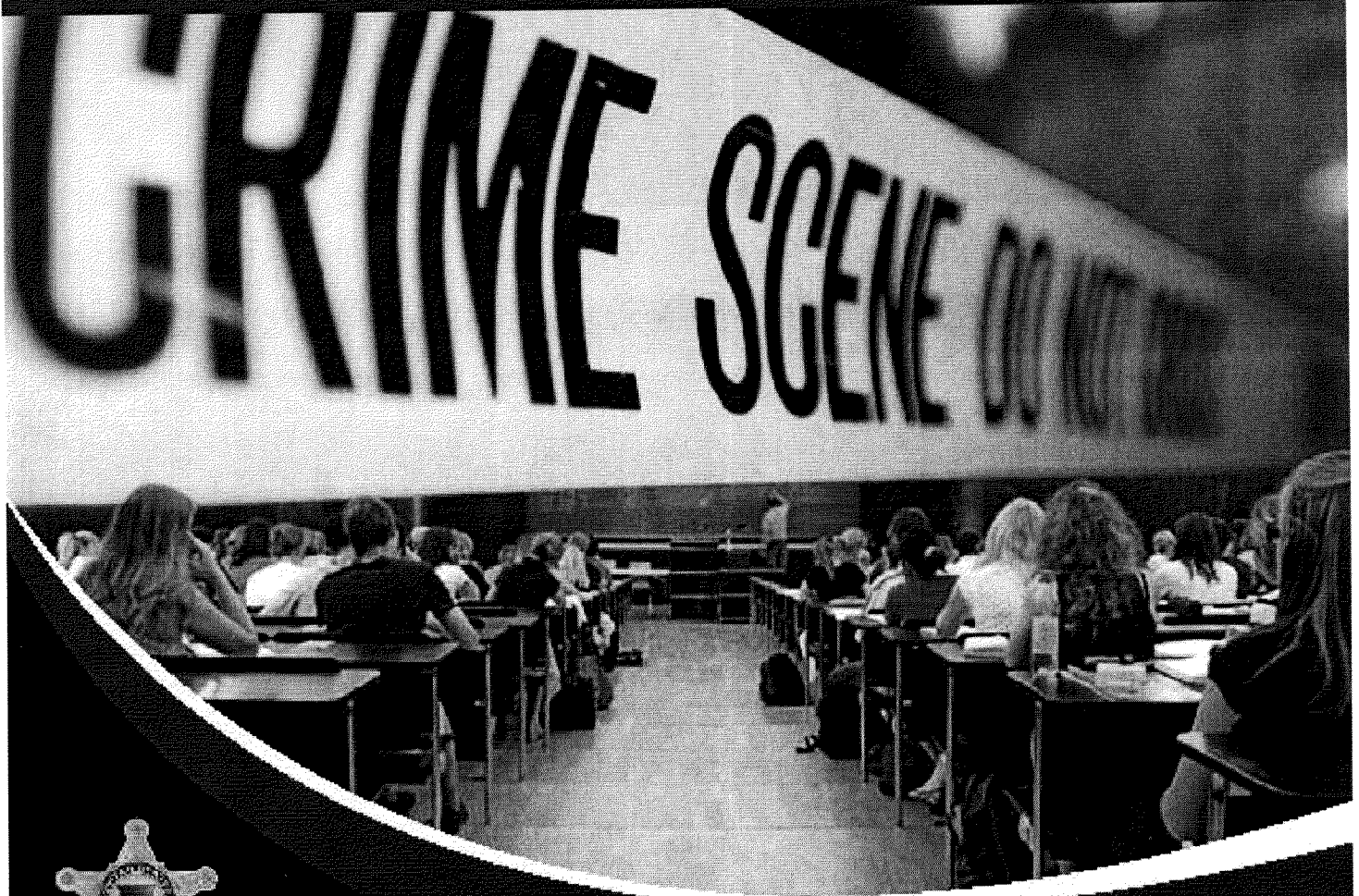
- [www.fbi.gov](http://www.fbi.gov)
- [www.safetyzone.org](http://www.safetyzone.org) (DOE and DOJ)
- [www.ncjrs.org/school\\_safety](http://www.ncjrs.org/school_safety)
- [www.ed.gov/offices/OESE/SDFS](http://www.ed.gov/offices/OESE/SDFS)
- [www.secretservice.gov/ntac.htm](http://www.secretservice.gov/ntac.htm)
- [www.keepschoolssafe.org](http://www.keepschoolssafe.org)

Information compiled from the *Safe School Initiative Report*, United States Secret Service and Department of Education, (2002); *School Violence Threat Management*, Dr. Kris Mohandie, (2000); *The School Shooter: A Threat Assessment Perspective*, CIRG/NCAVC, (1999).



# CAMPUS ATTACKS

Targeted Violence Affecting Institutions  
of Higher Education



April 2010

United States Secret Service • United States Department of Education • Federal Bureau of Investigation



**CAMPUS ATTACKS**  
**TARGETED VIOLENCE AFFECTING INSTITUTIONS OF HIGHER EDUCATION**

**United States Secret Service**  
**United States Department of Education**  
**Federal Bureau of Investigation**

*by*

**Diana A. Drysdale**  
**Lead Social Science Research Specialist**  
**National Threat Assessment Center**  
**United States Secret Service**

**William Modzeleski**  
**Associate Assistant Deputy Secretary**  
**Office of Safe and Drug-Free Schools**  
**Department of Education**

**Andre B. Simons**  
**Supervisory Special Agent**  
**Behavioral Analysis Unit**  
**Federal Bureau of Investigation**

**Washington, D.C.**  
**April 2010**



**U.S. Department of Homeland Security**

Janet Napolitano

*Secretary*

**U.S. Secret Service**

Mark Sullivan

*Director*

**U.S. Department of Education**

Arne Duncan

*Secretary*

**Office of Safe and Drug-Free Schools**

Kevin Jennings

*Assistant Deputy Secretary*

**U.S. Department of Justice**

Eric Holder

*Attorney General*

**Federal Bureau of Investigation**

Robert S. Mueller, III

*Director*

April 2010

This publication is in the public domain. Authorization to reproduce this publication in whole or in part is granted. While permission to reprint is not necessary, the citation should be: Drysdale, D., Modzeleski, W., and Simons, A. (2010). *Campus Attacks: Targeted Violence Affecting Institutions of Higher Education*. U.S. Secret Service, U.S. Department of Homeland Security, Office of Safe and Drug-Free Schools, U.S. Department of Education, and Federal Bureau of Investigation, U.S. Department of Justice. Washington, D.C., 2010.

This publication can be downloaded from the World Wide Web at the following URLs:

<http://www.secretservice.gov/ntac.shtml>

<http://www2.ed.gov/about/offices/list/osdfs/resources.html>

<http://www.fbi.gov/publications/campus/campus.pdf>

On request, this publication is available in alternate formats, such as Braille, large print, or computer diskette. For more information, please contact the Department's Alternate Format Center at 202-260-0852 or 202-260-0818.



## **A JOINT MESSAGE FROM THE U.S. SECRET SERVICE, THE U.S. DEPARTMENT OF EDUCATION, AND THE FEDERAL BUREAU OF INVESTIGATION**

In response to the Virginia Tech incident on April 16, 2007, former cabinet Secretaries Michael Leavitt and Margaret Spellings, and former Attorney General Alberto Gonzales submitted the *Report to the President on Issues Raised by the Virginia Tech Tragedy* dated June 13, 2007. The report included a recommendation that the U.S. Secret Service (Secret Service), the U.S. Department of Education, and the Federal Bureau of Investigation (FBI) explore the issue of violence at institutions of higher education (IHEs). Accordingly, we initiated a collaborative effort to understand the nature of this violence and identify ways of preventing future attacks that would affect our nation's colleges and universities.

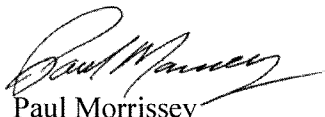
This effort was implemented through the Secret Service's National Threat Assessment Center, the Department of Education's Office of Safe and Drug-Free Schools, and the FBI's Behavioral Analysis Unit. The project drew from the Secret Service's experience in studying threat assessment and the prevention of targeted violence; the Department of Education's expertise in helping schools facilitate learning through the creation of safe environments for students, faculty, and staff; and, the FBI's threat assessment and investigative expertise.

The goal of this collaborative endeavor was to understand the scope of the problem of targeted violence at IHEs. To that end, this report offers preliminary findings from a review of 272 incidents of violence that affected IHEs in the United States from 1900 through 2008. We addressed fundamental questions regarding where, when, and how these incidents occurred, and captured information concerning the offenders and their relationship to the IHEs. When possible, we also identified factors that may have motivated or triggered the attacks.

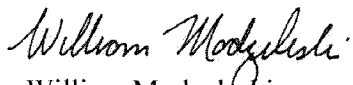
We strived to create a product that will be useful for threat assessment and campus safety professionals charged with identifying, assessing, and managing violence risk at IHEs. These law enforcement, mental health, student affairs, and legal professionals provide an incredible service under unique and often challenging circumstances. Ensuring the safety of college and university communities—some of which resemble small cities—is a daunting task. Navigating the intricacies of privacy laws, preserving academic freedoms, complying with civil rights laws, and simultaneously ensuring a safe campus and workplace environment are tasks not easily accomplished. We hope that this preliminary report contributes to that effort.



The Secret Service, the Department of Education, and the FBI are keenly aware of the profound and devastating physical, emotional, and psychological injuries that result from acts of violence against IHE community members and their effect on the nation as a whole. Through our collaboration, we are working to better understand what drives individuals to carry out acts of violence and ultimately how to prevent them in the future.



Paul Morrissey  
Assistant Director  
Office of Protective Research  
United States Secret Service



William Modzeleski  
Associate Assistant Deputy Secretary  
Office of Safe and Drug-Free Schools  
Department of Education



Robert A. Blecksmith  
Assistant Director  
Critical Incident Response Group  
Federal Bureau of Investigation



## **Acknowledgements**

The authors would like to thank project staff from each of the participating agencies for their invaluable contributions. At the U.S. Secret Service's National Threat Assessment Center (NTAC), these individuals include: Michelle Keeney, J.D., Ph.D., Lina Alathari, Ph.D., Eileen Kowalski, Tracey Mullins, Sergeant Rolanda Brodie, and Sergeant Timothy Burns. For the U.S. Department of Education's Office of Safe and Drug-Free Schools, these individuals include: Elizabeth Argeris, Deborah Rudy, and Tara Hill. The authors would also like to thank Kari DeCelle of the U.S. Department of Education's Readiness and Emergency Management for Schools Technical Assistance Center (REMS TA) for designing the cover. The Federal Bureau of Investigation's Behavioral Analysis Unit (BAU) would like to thank: Supervisory Special Agent (SSA) Shawn F. VanSlyke, Yvonne E. Muirhead, Katherine A. Schoeneman, Ph.D., Erin K. Nekvasil, and SSA David T. Resch. The BAU extends its gratitude to: Lesley A. Buckles, Helene V. Christensen, Allison Grupski, Meghann Hudson, Leigh Ann Perry, Kari L. Riddles, Kimberly C. Stamatopoulos, Elizabeth Sutton, and Maria Valdovinos.

This project also benefited from the thoughtful comments of a subject matter expert group comprising representatives from campus law enforcement, threat assessment professionals, and higher education. Participants included: Eugene Deisinger, Ph.D., Christopher Flynn, Ph.D., Steven J. Healy, Gary Lyle, Kris Mohandie, Ph.D., Mario J. Scalora, Ph.D., and Vasti Torres, Ph.D.



<b>INTRODUCTION.....</b>	<b>1</b>
<b>BACKGROUND .....</b>	<b>3</b>
<i>Previous incident-based research.....</i>	<i>3</i>
<i>Defining the IHE community.....</i>	<i>5</i>
<i>IHE campus crime .....</i>	<i>6</i>
<b>DEFINING AND IDENTIFYING THE INCIDENTS .....</b>	<b>8</b>
<i>Inclusion criteria.....</i>	<i>8</i>
<i>Methodology and limitations .....</i>	<i>9</i>
<b>THE FINDINGS.....</b>	<b>11</b>
<i>Where in the United States did the incidents occur? .....</i>	<i>11</i>
<i>When did the incidents occur? .....</i>	<i>11</i>
<i>Where did the incidents occur in relation to the IHE? .....</i>	<i>13</i>
<i>Who were the subjects?.....</i>	<i>15</i>
<i>What were the subjects' affiliations with the IHEs? .....</i>	<i>16</i>
<i>What method of attack was used? .....</i>	<i>17</i>
<i>Whom did the subjects harm? .....</i>	<i>17</i>
<b>QUALITATIVE OBSERVATIONS .....</b>	<b>18</b>
<i>What factors motivated or triggered the attacks? .....</i>	<i>18</i>
<i>How did target selection compare with the actual victims? .....</i>	<i>19</i>
<i>Targeting: Specifically Named Individuals.....</i>	<i>19</i>
<i>Targeting: Random Individuals .....</i>	<i>20</i>
<i>What pre-incident behaviors were directed toward the targets? .....</i>	<i>21</i>
<i>Verbal/Written Threats .....</i>	<i>21</i>
<i>Stalking/Harassment.....</i>	<i>22</i>
<i>Physically Aggressive Acts .....</i>	<i>22</i>
<i>Did others observe concerning behaviors just prior to the incidents?.....</i>	<i>22</i>
<b>CONSIDERATIONS .....</b>	<b>24</b>
<i>General observations.....</i>	<i>24</i>
<i>Diversity of the subject population .....</i>	<i>25</i>
<i>Diversity of criminal and other concerning behaviors.....</i>	<i>25</i>
<b>CONCLUSION .....</b>	<b>27</b>
<b>APPENDIX A: IHE DEFINITIONS.....</b>	<b>29</b>
<b>APPENDIX B: ADDITIONAL EXAMPLES OF INCIDENTS.....</b>	<b>30</b>
<b>APPENDIX C: DEFINITIONS OF INCIDENT CATEGORIES.....</b>	<b>33</b>



## INTRODUCTION

On April 16, 2007, Seung Hui Cho, 23, a student at Virginia Polytechnic Institute and State University ("Virginia Tech") in Blacksburg, Virginia, carried out what would become one of the deadliest school shootings in the world. Around 7:15 a.m., Cho fatally shot a female student in her dormitory room in West Ambler Johnston Residential Hall and then shot the building's residential advisor. Approximately two-and-a-half hours later, Cho entered Norris Hall, a lecture building, and shot numerous students and faculty before killing himself. In total, Cho killed 32 (27 students and five faculty members) and wounded 17. Some of the wounded individuals were struck by gunfire while others were injured trying to jump from the building.

This killing spree stunned the nation and questions echoed throughout the country from parents, administrators, and government officials alike. In response, Virginia Governor Timothy Kaine established the Virginia Tech Review Panel (VTRP) on June 18, 2007, to gain a better understanding of the incident and its underlying causes so that steps could be taken to minimize the chances of a similar tragedy happening again.<sup>1</sup>

At the federal level, President George W. Bush charged Attorney General Alberto Gonzales, Department of Education Secretary Margaret Spellings, and Department of Health and Human Services Secretary Michael Leavitt to convene meetings throughout the country focused on the issues raised by the Virginia Tech tragedy. Meetings were subsequently held with college and university representatives, local and state leaders, law enforcement officials, and mental health care providers. President Bush instructed Secretary Leavitt to summarize the lessons learned from these meetings and to recommend how the federal government could help prevent similar incidents in the future.

On June 13, 2007, based upon the meeting discussions as well as other input, the *Report to the President on Issues Raised by the Virginia Tech Tragedy* was issued.<sup>2</sup> This report presented a series of findings, common themes, observations, and recommendations, one of which stated: "The U.S. Department of Education, in collaboration with the U.S. Secret Service and the Department of Justice, should explore research of targeted violence in institutions of higher education and continue to share existing threat assessment methodology with interested institutions."<sup>3,4</sup> To that end, representatives from the U.S. Secret Service (Secret Service), the U.S. Department of Education, and the Federal Bureau of Investigation (FBI) initiated a partnership in pursuit of this goal.

The three entities began by asking fundamental questions, such as: How prevalent are the incidents of targeted violence that affect institutions of higher education (IHEs)? Who are the

---

<sup>1</sup> Virginia Tech Review Panel. (2007, August). *Mass shootings at Virginia Tech, April 16, 2007: Report of the Review Panel*. Retrieved July 8, 2008, from [www.vtreviewpanel.org/report/index.html](http://www.vtreviewpanel.org/report/index.html).

<sup>2</sup> U.S. Department of Health and Human Services. (2007, June 13). *Report to the President on issues raised by the Virginia Tech tragedy*. Retrieved August 21, 2008, from <http://www.hhs.gov/vtreport.html#intro>. Hereafter referred to as the "Report to the President."

<sup>3</sup> "Targeted violence" is defined as an incident of violence where a known or knowable attacker selects a particular target prior to their violent attack. See Fein, R.A., Vossekuil, B., & Holden, G. (1995, September). Threat assessment: An approach to prevent targeted violence. *Research in Action (NCJ 155000)*. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

<sup>4</sup> *Report to the President*, p. 9.



perpetrators? Are they affiliated with the affected IHE? There was limited previous research on these issues, so the initial framework for the project became clear to the three agencies, which began a comprehensive effort to identify, through open-sources, incidents of targeted violence that have affected IHE communities.

This report provides an overview of these incidents and the involved subjects, discusses initial observations regarding behaviors of the subjects, and offers preliminary considerations regarding the data that may have relevance to threat assessment. While the participating agencies are aware of the limitations of an open-source descriptive review, this preliminary effort will be complemented by a more in-depth study to be conducted by the Department of Education and the FBI.



## BACKGROUND

The specific phenomenon of targeted violence at institutions of higher education (IHEs) should be considered within its own context. This section begins by reviewing the previous incident-based research, defining the IHE community, and discussing what forms of criminal activity exist within this community.

### *Previous Incident-Based Research*

To better understand the breadth of issues with which an IHE may be confronted as part of a threat assessment, the Secret Service, Department of Education, and the FBI sought to identify and review literature that specifically examined the full-range of incidents of targeted violence affecting IHEs.

As noted by former Secretary Spellings, along with former Attorney General Gonzales and former Secretary Leavitt, a number of law enforcement officers, mental health care providers, school officials, and educators have cited the publication, *Threat Assessment in Schools: A Guide to Managing Threatening Situations and to Creating Safe School Climates*.<sup>5</sup> This guide was published jointly by the Secret Service and the Department of Education in May 2002. It was based upon the Safe School Initiative (SSI), a research project that examined 37 incidents of targeted school shootings that occurred between 1974 and 2000 at elementary, middle, and high schools. This landmark study identified observable pre-attack behaviors of student perpetrators in K-12 schools and highlighted several strategies for recognizing and managing persons who pose a threat to school populations.

When considering whether these findings are applicable to similar incidents within an IHE setting, it is important to note that specific and observable pre-attack behaviors demonstrated by attackers at the college or university level have yet to be thoroughly examined for comparison. Applying the findings of the SSI to IHE-based populations may provide appropriate prompts and insights to guide threat assessment, but there are important differences that may impact the threat assessment process.

At a basic level, the physical environment of a K-12 setting is vastly different from that of a college or university setting. Secondary schools typically comprise one to several buildings, utilize smaller classrooms, and provide an experience in which students have regular contact with the same faculty and staff. Communication between responsible parties regarding issues facing the student population is facilitated by this proximity. For the most part, numerous educators are aware of students' whereabouts and behaviors during each school day. Additionally, faculty meetings enable information sharing and increase the likelihood of recognizing behaviors of concern. In contrast, IHE campuses usually comprise many buildings, often with larger classrooms, separate faculty for each department, more uncontrolled access and egress, and irregular student schedules that minimize regular contact between educators and

---

<sup>5</sup> Fein, R., Vossekuil, B., Borum, R., Pollack, W. S., Modzeleski, W., and Reddy, M. (2002, May). *Threat assessment in schools: A guide to managing threatening situations and to creating safe school climates*. Washington, DC: United States Secret Service and United States Department of Education.



students. These factors are less conducive to observing and recognizing behavioral concerns among the student population.

At a more nuanced level, the developmental and social differences between high school students and college students suggest that IHE-based subjects may engage in pre-attack behaviors that differ from those of their high school counterparts. A college or university campus may be both an educational and a residential environment, making it a setting in which significant developmental and transitional stressors are ushered into a person's life. This combination is not often found in other settings. For the student who has just moved away from home, there are numerous environmental changes that can introduce a new dimension of stress. Some challenges include establishing self-sufficiency and responsibility, academic pressures, social pressures, and personal health and safety decisions. The student's coping skills can range from positive, such as seeking counseling or talking with friends, to negative, such as social withdrawal and isolation or alcohol and drug abuse.

When behaviors of concern are identified among secondary school students, there exists the potential for educators and threat assessment personnel to communicate with parents to solicit family involvement. However, options for the IHE official are more limited, as regular communication with parents is less likely to occur for a variety of reasons and IHE students who live away from home must reach out for services independently.

Beyond the SSI, there is limited research on IHE-related targeted violence that contains comprehensive incident analysis. The majority of the literature offers practical guidance on conducting threat assessments, preventing targeted violence, and handling the aftermath of an incident. There is some research on handfuls of incidents across all educational levels, not just IHEs, and in-depth case analyses focused on only a few incidents. The research has also addressed particular aspects of violence on IHE campuses, such as stalking, domestic violence, courtship violence, campus sexual assault, hazing, and drug/alcohol induced violence. Various surveys have been published that attempt to assess the frequency of violent crime affecting IHE communities. However, these surveys collected limited information and were focused on specific campuses, geographical areas, and timeframes. The relevance of this information is not in question, but the existing literature has generally looked at these issues in isolation and does not allow us to look across types of violence to gauge the relative prevalence and context.

One of the few reports to look across the spectrum was Max L. Bromley's *Campus-Related Murders: A Content Analysis Review of News Articles*.<sup>6</sup> Bromley examined *Chronicle of Higher Education* articles from 1989 to 2001 for incidents of campus murder to gain a deeper understanding of the offenders, victims, circumstances, and university or college response. Analysis of 33 incidents highlighted the fact that college campuses share commonalities with the communities at large with regard to murders. As in the general population, Bromley found, examples of domestic, intimate, and workplace violence were present in campus homicide cases. In a majority of the studied cases, there was some kind of relationship between the offender and the victim, and both tended to be members of the campus community (students, faculty, or staff).

---

<sup>6</sup> Bromley, M. L. (2005). *Campus-related murders: A content analysis review of news articles*. Paper presented at the Annual Conference of the Southern Criminal Justice Association. Retrieved September 25, 2008, from <http://www.dcf.state.fl.us> Updated link retrieved on April 14, 2010: [http://www.dcf.state.fl.us/initiatives/campussecurity/docs/Campus\\_Related\\_Murders050907.pdf](http://www.dcf.state.fl.us/initiatives/campussecurity/docs/Campus_Related_Murders050907.pdf).



Handguns and other weapons were used in about half of the campus murders, which mirrored the rate of murders involving handguns in the general community. Bromley noted that, despite these shared features, “little is known at this time about the nature and characteristics of murders on campus.”

As the professional literature does not offer a comprehensive perspective that examines the full-range of incidents faced by IHEs, the search focused on published lists of incidents of school-related violence. These lists typically reflected the following limitations: (1) the manner in which they were compiled was not always documented; (2) they lacked stated and clearly defined criteria for the inclusion of incidents; (3) they blended incidents from all educational levels (i.e., elementary, secondary, and postsecondary); (4) they often combined incidents that occurred within the United States and those that occurred on foreign soil; (5) they frequently focused on the more well-known incidents; and (6) they presented only basic information about each incident, such as the date, location, name of the subjects and/or victims, and a brief description of what occurred.

A review of the existing literature and resources confirmed the need for the Secret Service, the Department of Education, and the FBI to compile a comprehensive inventory of targeted violence incidents that have affected IHE communities.

### ***Defining the IHE Community***

According to the *Digest of Education Statistics: 2008 (The Digest)*,<sup>7</sup> there were 6,563 postsecondary Title IV Institutions in 2006-07.<sup>8</sup> Of these institutions, 4,314 were degree-granting<sup>9</sup> and 2,222 were non-degree-granting.<sup>10</sup>

Focusing primarily on the 4,314 degree-granting institutions, 2,629 (approximately 60 percent) were four-year colleges or universities, and 1,685 (approximately 40 percent) were two-year colleges. Student enrollment in these institutions in the fall of 2006 measured 17.8 million (11.2 million in four-year institutions and 6.5 million in two-year institutions).<sup>11, 12</sup> Of these students,

---

<sup>7</sup> Snyder, T.D., Dillow, S.A., and Hoffman, C.M. (2009, March). *Digest of Education Statistics 2008 (NCES 2009-020)*. Washington, DC: National Center for Education Statistics, Institute of Education Sciences, U.S. Department of Education. Retrieved June 1, 2009, from <http://nces.ed.gov>. Hereafter referred to as “The Digest.”

<sup>8</sup> Title IV institutions are defined as “all post-secondary institutions whose students are eligible to participate in the Title IV federal financial aid programs.” Table 5. Number of educational institutions, by level and control of institution: Selected years, 1980–81 through 2006–07, *The Digest*, p. 19.

<sup>9</sup> Degree-granting institutions are defined as “postsecondary institutions that grant an associate’s or higher degree and whose students are eligible to participate in the Title IV federal financial aid programs. Degree-granting institutions include almost all 2- and 4-year colleges and universities; they exclude institutions offering only vocational programs of less than 2 years duration and continuing education programs.” *The Digest*, p. 269.

<sup>10</sup> Non-degree granting included institutions that “did not offer accredited 4-year or 2-year degree programs, but were participating in Title IV federal financial aid programs. Includes some schools with non-accredited degree programs.” *The Digest*, p. 269.

<sup>11</sup> Table 186. Enrollment, staff, and degrees conferred in postsecondary institutions participating in Title IV programs, by type and control of institution, sex of student, type of staff, and type of degree: fall 2005, fall 2006, and 2006–07. *The Digest*, p. 276.

<sup>12</sup> These numbers may not equal the 17.8 million shown due to rounding. Not included in these numbers were an additional 446,604 students enrolled in non-degree-granting institutions.



42.7 percent were male and 57.3 percent were female. The youngest enrolled students were reported to be age 14; however, ages beyond 35 were not specified (see Table 1).<sup>13</sup>

The majority of the enrolled students in the fall of 2006 attended larger colleges and universities. Specifically, campuses boasting enrollment levels of 10,000 students or more represented only 12 percent of the institutions; however, they enrolled 55 percent of all college students.<sup>14</sup> By comparison, 41 percent of the institutions had enrollment levels of less than 1,000 students, and these institutions enrolled only 4 percent of all college students.

In addition to students, IHE communities comprise employees that include faculty, administration, and support staff. In the fall of 2007, 3.6 million people were employed at degree-granting institutions.<sup>15</sup> This number includes 2.6 million professional staff (including faculty, executive/administrative/ managerial personnel, graduate assistants, and other professionals) and 932,027 non-professional staff (including technical/clerical/secretarial personnel, skilled trade persons, and maintenance staff). Sixty-four percent of the employees worked on a full-time basis, while the remaining 36 percent were part-time. Overall, the employee population was 46 percent male and 54 percent female.<sup>16</sup> Age distributions were not reported.

**Table 1: Student Enrollment, by Age Group, Fall 2006**

Age	Enrollment	%
14-17	231,000	1.3
18-19	3,769,000	21.2
20-21	3,648,000	20.5
22-24	3,193,000	18.0
25-29	2,401,000	13.5
30-34	1,409,000	7.9
Over 35	3,107,000	17.5
Total	17,758,000	100

### ***IHE Campus Crime***

Maintaining the safety of IHEs and the students and employees that comprise IHE communities is a vital task. The statistics reported as part of the *Crime Awareness and Campus Security Act of 1990* offer a gauge of the level and type of crime that takes place on college campuses. Amended three times in 1992, 1998, and 2000, this act was renamed in 1998 the *Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act*, or the *Clery Act*, in memory of a student who was killed in her dormitory room in 1986. In response to the Virginia Tech shootings, Congress further amended the act in 2008, adding a campus emergency response plan to its requirements. The amendment requires IHEs to “immediately notify” the campus community as soon as an emergency is confirmed on the campus unless such notification would impede attempts to control the situation.

The *Clery Act* requires all colleges and universities that participate in the federal financial aid programs under Title IV of the *Higher Education Act* to maintain and disclose information about certain crimes committed on or near campuses. The *Clery Act* defines these crimes as they are defined in the FBI’s Uniform Crime Reporting Handbook (UCR).

Specifically, campus personnel must track and report criminal homicides, including murder, negligent and non-negligent manslaughter, sex offenses (including forcible and non-forcible),

<sup>13</sup> Table 190. Total fall enrollment in degree-granting institutions, by sex, age, and attendance status: Selected years, 1970 through 2017. *The Digest*, p. 280.

<sup>14</sup> *The Digest*, p. 270.

<sup>15</sup> Statistics were reported for fall 2005 and fall 2007 only.

<sup>16</sup> Table 243. Employees in degree-granting institutions, by sex, employment status, control and type of institution, and primary occupation: Selected years, fall 1987 through fall 2007. *The Digest*, p. 358.



robbery, aggravated assault, burglary, motor vehicle theft, and arson. They must also report whether any of these crimes, other crimes involving bodily harm, or larceny, theft, simple assault, intimidation, and destruction, damage or vandalism of property were hate crimes. Statistics are also required for arrests and disciplinary action referrals for weapons possession or drug and alcohol law violations.

Under the *Clery Act*, criminal activity must also be broken down by location, whether “on campus, in or on a non-campus building or property, or on public property within or immediately adjacent to and accessible from the campus.”<sup>17</sup> Finally, the *Clery Act* does not make any distinction regarding the resolution of the reported crimes (unless deemed to be unfounded by law enforcement) and does not limit the reported crimes to those that affected or were committed by IHE students or employees.

Table 2 depicts the number of crimes reported to the Department of Education in compliance with the *Clery Act* from 2005 through 2008.<sup>18</sup> Data were reported by public and private institutions ranging from four-year and above to less than two-year. Those institutions with multiple campuses reported data for each campus. Looking at all 235,599 crimes reported over this timeframe, 74.6 percent were burglaries and motor vehicle thefts, 9.2 percent were aggravated assaults, 8.4 percent were robberies, 5.9 percent were forcible sex offenses, 1.7 percent were arsons, and 0.1 percent were non-forcible sex offenses. The remaining 0.1 percent of reported crimes were murders and non-negligent manslaughter (0.07 percent,  $n = 174$ ) and negligent manslaughter (0.02 percent,  $n = 46$ ).<sup>19</sup> Of the 174 murders and non-negligent manslaughters, 80 occurred on campus (13 of which took place in residence halls), 82 occurred on public property immediately adjacent to campuses, and 12 occurred at non-campus facilities.

**Table 2: Crime Statistics Reported in Compliance with the *Clery Act*, by Type of Crime and Year: 2005-08**

	Murder / Non- Negligent Manslaughter	Negligent Manslaughter	Forcible Sex Offense	Non- Forcible Sex Offense	Robbery	Aggravated Assault	Burglary	Motor Vehicle Theft	Arson
2005	28	33	3,583	55	5,432	5,943	37,800	11,890	1,219
2006	25	0	3,490	56	4,921	5,472	35,124	9,811	1,086
2007	66	8	3,482	62	4,985	5,234	33,010	8,744	915
2008	55	5	3,287	49	4,562	5,026	31,851	7,465	825
Total	174	46	13,842	222	19,900	21,675	137,785	37,910	4,045

Although murder and non-negligent homicide represent the second smallest percentage of crimes reported by campus officials, the prevention of these types of crimes is a priority among IHE officials. The current effort between the Secret Service, the Department of Education, and the FBI seeks to identify for study a subset of these crimes—that is, incidents of targeted violence—to support prevention efforts.

<sup>17</sup> U.S. Department of Education, Office of Postsecondary Education. (2005, June). The handbook for campus crime reporting, p. 11. Retrieved September 25, 2008, from <http://www.ed.gov/admins/lead/safety/handbook.pdf>. Also see Higher Education Act, 34 C.F.R. 668.46(a) for full definitions of campus, and public property.

<sup>18</sup> U.S. Department of Education, Office of Postsecondary Education. (n.d.) The campus security data analysis cutting tool, aggregated data for calendar years 2005-07 and 2006-2008 [spreadsheets]. Retrieved July 22, 2009, from <http://ope.ed.gov/security/>. Numbers shown for 2005 were taken from the aggregate data for 2005-07. Numbers shown for 2006-08 were taken from the aggregate data for 2006-08.

<sup>19</sup> These numbers may not equal the 0.1 percent shown due to rounding.



## DEFINING AND IDENTIFYING THE INCIDENTS

The partner agencies designed and launched an effort to identify a broad range of incidents that have affected IHEs. The goal of this effort was to identify relevant incidents involving directed assaults and to gather information on the key incident elements that could be gleaned from open-source reporting. To ensure that the scope encompassed the many issues that an IHE may face, incidents affecting postsecondary vocational and proprietary schools were also included.<sup>20</sup>

### *Inclusion Criteria*

Criteria were determined in advance to guide the selection of incidents for inclusion. As the term “targeted violence” lacks the degree of specificity necessary for incident criteria, for the purposes of this report, we have selected and defined a more precise term that will reflect the full spectrum of incidents. Relevant incidents were defined as **directed assaults** in which open-source reporting suggested they met the following four criteria:

- (a) The Target(s):
  - (1) The subject(s) selected a *specific* IHE Student(s), IHE Employee(s), or IHE Facility/Event(s) as a target (see Appendix A for definitions), or
  - (2) The subject(s) selected a *random* IHE Student(s), IHE Employee(s), or IHE Facility/Event(s) because the target’s characteristics matched the subject’s victim profile.<sup>21</sup>
- (b) Timing of Target Selection:
  - (1) The target(s) was selected *prior to the initiation of the assault*, or
  - (2) The target(s) was selected *at the time of the assault* based on a victim profile or the subject’s personal pre-existing relationship with the target(s) (e.g., roommates, friends, romantics).
- (c) Lethality of Assault: The subject(s) *employed or had the present ability to employ lethal force*.<sup>22</sup>
- (d) Timeframe and Geographical Limitations:
  - (1) The incident occurred between *January 1, 1900*<sup>23</sup> *and December 31, 2008*,
  - (2) The incident occurred **on-campus, off-campus**, or in/around a **non-campus** facility (see additional criteria below; see Appendix A for definitions), and
  - (3) The incident occurred *within the United States*.

---

<sup>20</sup> The question of whether the affected IHEs were Title IV institutions or degree-granting was set aside for case identification purposes as the Title IV designation was not in effect until after the passage of *The Higher Education Act of 1965* and the accreditation status of particular schools evolved over time.

<sup>21</sup> “Victim profile” is defined as a set of demographic or other perceived static traits that the subject(s) sought in selecting a target(s). Example: A subject goes to an IHE campus looking for a blond college-aged female to abduct and kill as part of a fantasy.

<sup>22</sup> “Lethal” is defined as causing or capable of causing death. Crimes of a sexual nature were included only if the subject actually employed lethal physical force.

<sup>23</sup> Due to the limited availability of searchable media reporting prior to 1900, this year was selected as the start date.



For incidents that took place off-campus and involved two persons in a romantic, spousal, or co-habitant/roommate relationship, both the subject and the target must have been affiliated with the affected IHE, with at least one of their affiliations current.

In general, incidents that fell within any of the following areas were excluded: hazing, pranks, crimes primarily motivated by material gain, murder-for-hire schemes connected to a separate crime, incidents perpetrated by ideological groups or arising from general social disorder, low-level assaults on facilities with little to no capacity to cause injuries or fatalities, gang and drug-related violence, spontaneous altercations between strangers, and incidents with insufficient information to determine whether they met the inclusion criteria. These latter incidents included those in which either the subject was not identified in open-source reports or the case remained unsolved at the time the research was performed. Additionally, incidents involving serial killers who were not formerly or currently affiliated with the affected IHE were also excluded.

### ***Methodology and Limitations***

Incidents were identified from open-source reporting via a three-step process. First, lists of school-related incidents of violence available on the Internet and published documents were reviewed. Thirty-one incidents from these previously compiled lists and publications met the definition of a directed assault. Second, a complex search string was developed and applied to the Nexis "All English News Group." Language used to describe the incidents identified in the first step served as the basis for the construction of this search string. Although news articles from 1970 through 2008 were reviewed, it is important to note that the media coverage contained in Nexis is sparse until the 1990s. After reviewing over 111,800 search results, an additional 198 incidents were identified that met the definition of a directed assault. Finally, a phrase-based search was executed in NewspaperArchive.com on available articles from 1759 through 1990. After screening over 3,600 search results, 43 additional incidents were identified that met criteria for inclusion. At the completion of this effort, it was determined that only those cases that took place from 1900 onward would be included due to the limitations of the press coverage prior to that year. The final sample consists of 272 incidents identified through this search process.

Data gathered for each incident included specific case information and qualitative observations. The specific case information fell within the categories of incident overview (e.g., date, location, type of IHE), incident specifics (e.g., site of attack, weapon used), subject descriptors (e.g., affiliation with IHE, gender, age), and incident outcome (e.g., injuries, deaths, judicial status). Data underwent a four-stage review process by a minimum of three researchers to verify the information gathered. Variables were created to capture the qualitative observations, which characterized the subject's apparent motives and triggers, targeting, and pre-incident behaviors. Two researchers independently coded these variables following a prescribed protocol. When necessary, additional research was performed to fill in gaps or clarify points using the three resources named above, Lexis-Nexis federal and state case law databases, and open Internet searches.

As all information obtained about the incidents was limited to open-source materials, it is important to emphasize a few of the limitations inherent in using such data for behavioral research. First, since this sample only includes those incidents that were reported in the media, it



is possible that there were other directed assaults at IHEs that met the inclusion criteria during the same timeframe. Second, as the level of detail reported varied significantly across incidents, data collected was limited to what could reasonably be collected for each case. Finally, we recognize that media reporting often contains objective and subjective errors. While the former are factual or mechanical in nature, the latter involve errors in the meaning or interpretation of the events.<sup>24</sup> When challenged with conflicting reports across sources, consideration was given to a number of factors, including the apparent quality of reporting, timing of the reporting, location of the media outlet in relation to the incident, and the source cited in the report. No efforts were made to check the veracity of reporting against primary sources other than when legal documents were available in Lexis. Given these limitations, the reader is reminded that this undertaking is purely descriptive, and is not comparative or predictive.

---

<sup>24</sup> Singletary, M. (1980, January 25). *Accuracy in the news reporting: A review of the research* (No. 25). Washington, DC: ANPA News Research Center. Retrieved on January 8, 2010, from [http://www.eric.ed.gov/ERICDocs/data/ericdocs2sql/content\\_storage\\_01/0000019b/80/32/9e/5b.pdf](http://www.eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/32/9e/5b.pdf); and, Maier, S. (2002). Getting it Right? Not in 59 Percent of Stories. *Newspaper Research Journal*, 23 (1). Retrieved on January 8, 2010, from <http://www.questia.com>.



## THE FINDINGS

Although the following results should be viewed in light of the limitations related to open-source reporting, this information does offer perspectives on the breadth and key aspects of the 272 incidents of targeted violence that serve as the basis for this report.

### *Where in the United States did the incidents occur?*

Incidents were identified in 42 states and the District of Columbia, with 57 percent ( $n = 155$ ) of the incidents affecting IHEs located in only 10 states,<sup>25</sup> eight of which are among the 10 states with the most IHEs.<sup>26</sup> The majority of the incidents affected IHEs designated as 4-year institutions (84 percent,  $n = 228$ ), followed by 2-year institutions (14 percent,  $n = 38$ ), postsecondary vocational/technical schools (1 percent,  $n = 4$ ), and those institutions identified as post-graduate only (1 percent,  $n = 2$ ).<sup>27</sup> In all, incidents affected 218 distinct campuses.

### *When did the incidents occur?*

Targeted violence affecting IHEs is not a new phenomenon (see Table 3). The first incident identified that met criteria occurred on April 29, 1909. On this date, a subject, who was not affiliated with the affected IHE, fatally shot his former girlfriend, a student, on her college campus. He then killed himself. The target had reportedly refused the subject's marriage proposals. He had come to the college two to three days earlier to persuade the target to change her mind.

The majority of incidents occurred during the 1990s and 2000s. It is unknown what may have caused the increase in incidents identified during the past 20 years. However, consideration should be given to the increased enrollment levels at IHEs as well as the increase in media coverage and digital reporting throughout the United States over the past few decades.

Figure 1 shows the increase in fall student enrollment levels at postsecondary, degree-granting institutions from 1909 through 2009 (projected).<sup>28</sup> It also shows the number of incidents identified by decade from the 1900s through the 2000s. Generally, as enrollment levels increased over time, so did the number of reported incidents.

**Table 3: Directed Assaults by Decade, 1900-2008**

Decade	<i>N</i> =	%
1900s	1	0.4
1910s	0	0.0
1920s	3	1.1
1930s	8	2.9
1940s	1	0.4
1950s	13	4.8
1960s	19	7.0
1970s	25	9.2
1980s	40	14.7
1990s	79	29.0
2000s*	83	30.5
Total	272	100.0

\* Data collected through 2008.

<sup>25</sup> From highest to lowest number of incidents, these 10 states are: California, New York, Texas, Florida, Michigan, Ohio, Pennsylvania, Illinois, Indiana, and North Carolina.

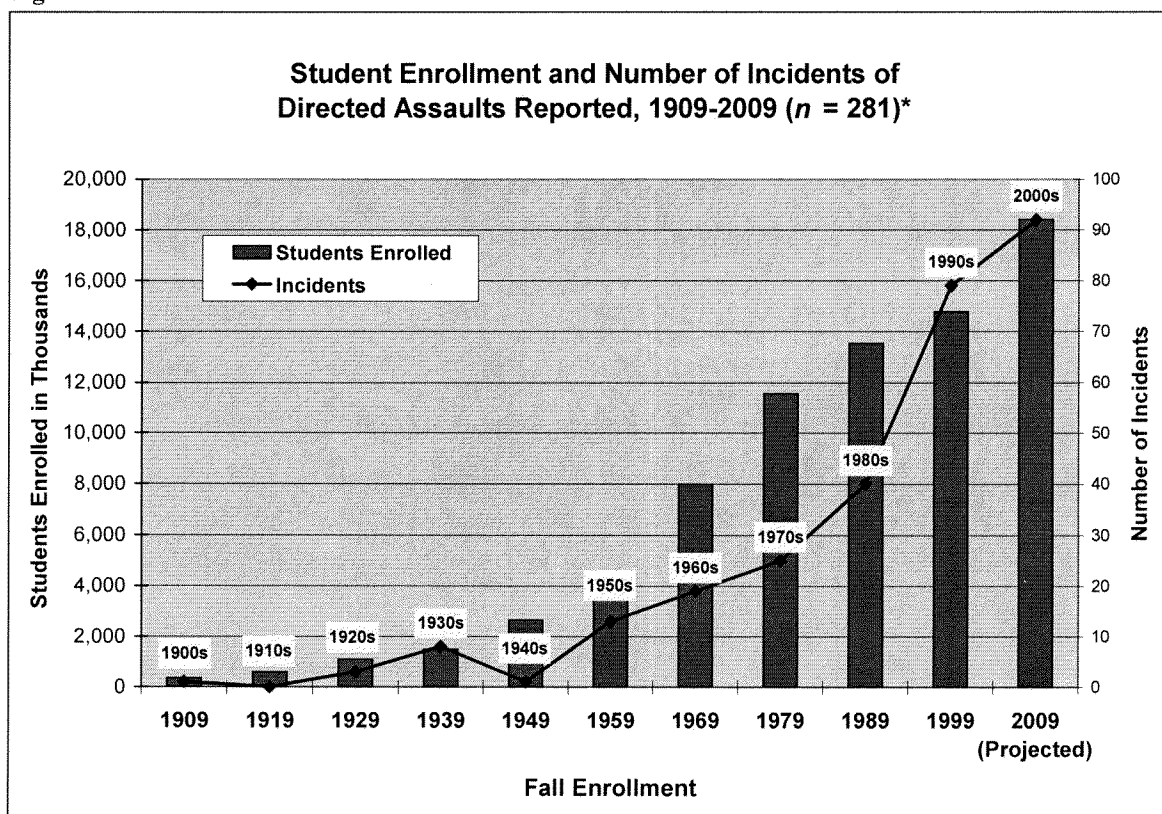
<sup>26</sup> Table 266: Degree-granting institutions and branches, by type and control of institution and state or jurisdiction: 2007–08. Of note, looking at the media sources searched in Lexis-Nexis, the largest resource used in identifying incidents, the states with the most incidents coincided with the states with the most newspapers and wire services.

<sup>27</sup> Percentages may add up to more than 100 percent due to rounding.

<sup>28</sup> Table 3. Enrollment in educational institutions, by level and control of institution: Selected years, 1869-70. *The Digest*, p. 16.



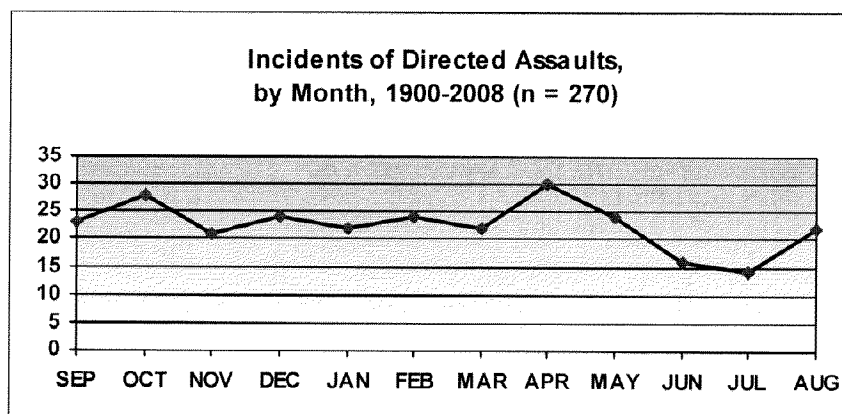
Figure 1



\*Data was collected through 2008 and projected for 2009 based on the average number of incidents observed per year from 2000 to 2008. Pearson ( $r = 0.924$ ,  $p < 0.000$ ) correlation is significant at the 0.01 level (1-tailed).

Incidents also occurred throughout the calendar year ( $n = 270$ ).<sup>29</sup> Figure 2 shows that although there was a decrease in the frequency, incidents happened even during the summer months.

Figure 2



<sup>29</sup> For two of the incidents, the months in which they occurred could not be determined from open-source reporting.



### *Where did the incidents occur in relation to the IHE?*

It may initially seem as though only incidents occurring on-campus are relevant to understanding targeted violence that affects IHEs. However, such a view neglects the role of campus safety departments and campus threat assessment teams in securing the area surrounding the campus and assessing the threats posed by and to IHE students, faculty, and staff, regardless of whether the ultimate act of violence occurs within the confines of the campus boundaries. Thus, the current project aimed to identify incidents that could fall within the purview of a campus threat assessment. A majority of the incidents occurred on-campus (79percent,  $n = 214$ ), while approximately one-fifth (19 percent,  $n = 52$ ) were off-campus. The remaining six incidents occurred either at non-campus<sup>30</sup> locations (1 percent,  $n = 3$ ) or at undetermined sites (1 percent,  $n = 3$ ).

Of those incidents that occurred at on-campus or non-campus sites ( $n = 217$ ), similar numbers of incidents took place in residential buildings (28 percent,  $n = 60$ ), parking lots or campus grounds (27 percent,  $n = 58$ ), and administrative and/or academic buildings such as offices, classrooms, laboratories (26 percent,  $n = 56$ ; see Table 4). In only 3 percent ( $n = 6$ ) of the on/non-campus incidents did the subject move from the campus grounds or parking lots to buildings, move between buildings, or cause injuries and/or deaths in more than one location on campus. In addition to the Virginia Tech attack in 2007, two other examples in which subjects moved from one location or building to another are the following:

**Table 4: On and Non-campus Directed Assaults, by Building, 1900-2008**

Buildings	$n =$	%
IHE Residence	60	27.7
IHE Grounds & Parking Lots	58	26.7
Administrative or Academic	56	25.8
Student/Employee Services	22	10.1
Other/Undetermined	15	6.9
Multiple Facilities/Buildings	6	2.8
Total	217	100.0

*On August 1, 1966, a 25-year-old student and former marine seized an observation tower on campus, killing and/or injuring several people on his way up the tower, then randomly fired a rifle at passersby for approximately 96 minutes. He was eventually shot by police. In the aftermath, 13 people were killed and 31 were wounded on the campus. The evening before the incident, the subject typed a final letter of explanation detailing his thoughts. He then went to his mother's home, choking and fatally stabbing her shortly after midnight. After writing another letter, which he left there, he returned home and fatally stabbed his wife as she slept. Penning notes to other family members, he prepared for his attack later that day.*

*On December 14, 1992, an 18-year-old student killed one professor, one student, and wounded four others in a random sweep across campus. The subject first approached a security-guard shack on the campus and shot the guard inside. Critically wounding him, he then fatally shot a professor, who was driving past. From there, he walked to the library where he fatally shot a student. He then entered a dormitory and resumed firing. He surrendered to police after his rifle jammed and he called 911, informing them that he was the shooter. Reportedly, the subject held views that were perceived as racist, homophobic and anti-Semitic by fellow students and was not adjusting well to the campus environment.*

*See Appendix B for descriptions of the remaining three incidents.*

<sup>30</sup> See Appendix A for definition.



Of the incidents that occurred within an IHE owned/operated building ( $n = 159$ ), over half of them took place in dorm rooms or apartments, offices, and instructional areas such as classrooms, lecture halls, or laboratories ( $n = 90$ , 57 percent; see Table 5).

**Table 5: Directed Assaults within IHE Buildings, by Locale, 1900-2008**

Locales	$n =$	%
Dorm Room or Apartment	48	30.2
Office(s)	22	13.8
Instructional Area	20	12.6
Non-specific/Other/Undetermined	16	10.1
Common Area	15	9.4
Hallway(s)/Stairwell(s)/Restroom(s)	15	9.4
Student Services Locales/Cafeteria	10	6.3
Multiple Locales within the Same Building	7	4.4
Multiple Facilities/Buildings	6	3.8
Total	159	100

Several subjects also carried out their attacks in multiple locales within the same building, moving from offices and classrooms to common areas, causing injuries and deaths at the different locales (4 percent,  $n = 7$ ). One example includes the following:

*On October 28, 2002, a 41-year-old student entered a college building shortly before 8:30 a.m., looking for three instructors. The subject fatally shot the first in her 2nd-floor office. He then fatally shot the second in a 4th-floor classroom in front of approximately 20 students, walked to the back of the classroom and shot his final victim. Soon after, he released the students and shot himself. The subject had been failing and had mailed a 22-page letter and other documents to a local media outlet. In his letter, he sketched his failed marriage, poor health, and the slights he perceived from the nursing school he claimed treated male students as "tokens."*

*See Appendix B for descriptions of remaining six incidents.*

In turning to those incidents that occurred off-campus ( $n = 52$ ), most took place at a private residence (75 percent,  $n = 39$ ), while approximately one-fifth of the incidents occurred outside of a structure (e.g., on a sidewalk, in a parking lot; 19 percent,  $n = 10$ ). Two examples of incidents that occurred off-campus include the following:

*On December 11, 1949, a 24-year-old student strangled his girlfriend, a fellow student, after a fraternity party at an off-campus men's rooming house. Two months prior, a university psychiatrist had treated the subject for suicidal ideations and an impulse to kill said girlfriend.*

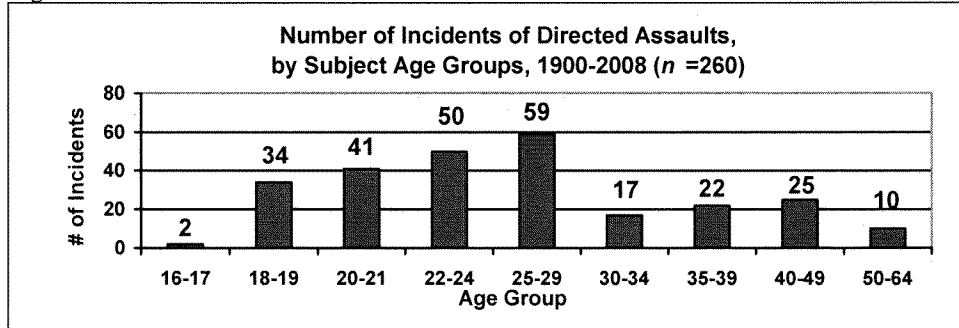
*On February 16, 2004, a 38-year-old former student who had worked for a psychology professor at a test center stalked her, went to her off-campus private residence, stabbed, and decapitated her. He then stripped off his clothing and ran in front of a truck on the highway, killing himself.*



### Who were the subjects?

Efforts were made to gather information regarding the subjects who carried out the attacks. The majority of incidents were perpetrated by one individual ( $n = 270$ ) and, of those, most of the subjects were male (94 percent,  $n = 254$ ).<sup>31</sup> In the incidents where age was reported ( $n = 260$ ), the range was 16 to 62, with an average age of 28 ( $Mdn = 25$ , mode = 20). See Figure 3 for a depiction of the number of incidents by subject age groups.

Figure 3



#### *The Youngest Subject:*

*On October 10, 1993, a 16-year-old male who was not affiliated with the affected IHE, detonated a pipe bomb outside the dorm room of two black students. Though no injuries were reported, the building was "severely damaged" by the racially motivated attack. The subject, who had tried to join a white supremacist organization, had admitted responsibility to witnesses and vowed to shoot all the black students at the college.*

#### *One of the Two Oldest Subjects:*

*On October 13, 2008, a 62-year-old, part-time librarian fatally shot a fellow full-time librarian, allegedly after a dispute the previous night over "work ethics." After the shooting, the subject sat down and calmly waited for police.*

Of note, among the cases there were three subjects who carried out multiple attacks on the same campus within a one to two month timeframe. An example includes the following incident:

*Beginning in December 1991, a 35-year-old former student, who had graduated 6 years prior, carried out two sniper-style attacks on his old campus. On December 12, 1991, the subject fatally shot a janitor in an auditorium. Then on January 29, 1992, he shot and wounded a female graduate student as she waited in a building for her husband. It was during a third similar incident that the subject was killed by police. On February 10, 1992, the subject was shooting at a student housing complex near the campus. After a foot pursuit, the subject was killed by police. Though he had been rejected from the graduate program four years prior, the motive for the attacks was not clear.*

*See Appendix B for descriptions of the remaining two incidents.*

<sup>31</sup> In two cases, the incidents were perpetrated by more than one subject so individual-level data regarding the subjects in those incidents were not gathered.



### What were the subjects' affiliations with the IHEs?

In addition to basic descriptive information, the subjects' affiliations with the affected IHEs were examined. A subject's primary affiliation with the IHE was designated as either a *direct* affiliation (e.g., current or former student or employee) or *indirect* affiliation (e.g., a spouse, other immediate family member, non-spouse intimate partner, or friend of a current IHE student or employee). In addition, if the subject was affiliated with the affected IHE in more than one way, the subject's primary affiliation was captured (e.g., a full-time student who worked part-time on-campus was designated as a student rather than an employee).

Of those cases in which this information was reported ( $n = 268$ ),<sup>32</sup> a majority of the subjects were identified as either current or former students at the affected IHE (60 percent,  $n = 161$ ), while approximately one-tenth were current or former employees of the IHE (11 percent,  $n = 29$ ). An additional 20 percent ( $n = 53$ ) of the subjects were indirectly affiliated with the IHE through a personal relationship with a current IHE student and/or employee. In less than one-tenth of the cases (9 percent,  $n = 25$ ), the subject had no known affiliation with the affected IHE. See Table 6 for additional information specific to each affiliation type.

**Table 6: Characteristics and Casualties Listed by Subjects' IHE Affiliation**

	Students ( <i>n</i> = 161)	Employees ( <i>n</i> = 29)	Indirectly Affiliated ( <i>n</i> = 53)	No Known ( <i>n</i> = 25)
<i>Gender</i>				
Male	93%	97%	96%	92%
Female	7%	3%	4%	8%
<i>Average Age</i>	25.5 ( <i>n</i> = 157)	38.7 ( <i>n</i> = 27)	29.9 ( <i>n</i> = 51)	27.4 ( <i>n</i> = 23)
Median	23	37	27	23
Mode	22	25 <sup>a</sup>	19 <sup>b</sup>	23
Range	17 to 62	18 to 62	18 to 55	16 to 51
<i>Status</i>				
Current	121	17	20	Not Applicable
Former	39	12	33	
Unknown	1	0	0	
<i>Affiliation Details</i>				
	Undergrad (62%) Graduate (18%) Alumni (8%) 2-year (6%) Voc/Technical (2%) Undetermined (5%)	Included range of positions, such as professors, librarians, security, janitorial, other.	60% ( <i>n</i> = 32) current or former non-spouse intimate partners. 15% ( <i>n</i> = 8) current or former spouses.	Not Applicable
<i>Casualties (excluding subjects)</i>				
Injuries	170	10	28	37
Deaths	193	27	37	22

<sup>a</sup> Multiple modes exist, smallest value is shown in Table 6 (25, 36, 37, 45).

<sup>b</sup> Multiple modes exist, smallest value is shown in Table 6 (19, 24).

<sup>32</sup> Multiple subject cases and those involving subjects whose affiliation could not be determined were excluded resulting in a total  $n$  of 268.



### ***What method of attack was used?***

Firearms were used most often (54 percent,  $n = 148$ ), followed by knives/bladed weapons (21 percent,  $n = 57$ ), a combination of weapons/methods (10 percent,  $n = 26$ ), and strangulation either manually or with an implement (5 percent,  $n = 14$ ). Of those incidents in which a combination of methods was used, most targets were strangled and stabbed. The remaining 27 incidents (10 percent) involved a blunt object, firebomb/incendiary/arson, explosives, poison, a vehicle, or a physical assault without a weapon.

### ***Whom did the subjects harm?***

Across all 272 incidents, the subjects caused 281 deaths and injured 247 individuals. Of the deaths, at least 190 were students and at least 72 were employees. Of the injured, at least 144 were students and at least 35 were employees. Not included in these numbers are the subjects themselves who were injured or killed either during or following the incident. In 26 percent ( $n = 71$ ) of the incidents, the subject died of a self-inflicted injury incurred during implementation of the assault or within hours or days of the incident. In 4 percent of the incidents ( $n = 11$ ), the subject survived his self-inflicted injuries and in an additional 4 percent of the incidents ( $n = 10$ ), the subject was killed by law enforcement during or immediately following the assault.



## QUALITATIVE OBSERVATIONS

Key elements of a thorough threat assessment include such items as the subject's motive and goal in carrying out an attack, triggering life events, target selection, and/or prior concerning or threatening behavior. These elements are at times difficult to discern due to the availability of information and subjectivity of their interpretation. Information related to these elements is particularly difficult to gather from open-sources, which do not always contain complete and accurate reporting.

Efforts were made to gather as much information as possible to provide an initial description of the motives and triggers, targeting, and pre-incident behaviors of concern. When the information was reported, judgments were made as to its completeness and apparent accuracy. A more in-depth analysis of each of these elements would require additional data other than what is available through open-source.

### *What factors motivated or triggered the attacks?*

Generally, several categories were observed among the incidents regarding the factors that may have played a role in the subjects' decision to carry out the directed assault. These factors fall broadly within areas related to personal relations, academic performance, workplace issues, and/or individual stressors (see Table 7; for definitions, see Appendix C). Although it was recognized that multiple factors may have motivated or triggered the offenders' violent acts, efforts were made to identify the most prominent ones and the incidents were categorized accordingly. In 17 percent ( $n = 45$ ) of the cases, either the motivating and/or triggering factors were completely unknown or they were less apparent as various factors specific to the subject and his/her environment appeared to influence the decision to engage in the violent behavior. Those incidents in which the motive and/or trigger was not apparent were excluded from Table 7.

**Table 7: Factors that Motivated or Triggered the Directed Assaults**

Categories	<i>n</i> =	%
Related to an Intimate Relationship	77	33.9
Retaliation for Specific Action(s)	31	13.7
Refused Advances or Obsession with the Target	23	10.1
Response to Academic Stress/Failure	23	10.1
Acquaintance/Stranger Based Sexual Violence	22	9.7
Psychotic Actions	18	7.9
Workplace Dismissal/Sanction	14	6.2
Need to Kill / Specific Victimology	7	3.1
Draw Attention to Self/Issue(s)	7	3.1
Bias Related	5	2.2
Total	227	100

As noted in Table 7, the most prevalent category identified related to current or former personal relationships between the subject and victim, followed by retaliation for specific actions. Future research should examine primary source materials, which may offer more insight into the underlying motives and triggers related to these incidents.



### *How did target selection compare with the actual victims?*

Regarding the subject's apparent targeting and scope of his or her victims, efforts were made to distinguish those subjects who had specific targets from those who did not, and then designate whether the actual victims who were injured or killed appeared to be the intended victims. Various items were taken into account when determining targeting, including the subject, the setting in which the subject was functioning, the context of the situation with which he or she was faced (e.g., relationship breakup, academic or work suspension, imminent or actual academic failure, loss of job, or delusions), and the subject's relationship to the target (e.g., current or former intimate partner, co-worker, professor, classmate, stranger). Additionally, consideration was given to the subject's reported actions before, during, and after the attack. Specific examples of factors considered in the decision-making process include the following:

- indications of planning,
- method and manner of the attack,
- travel by the subject to a locale where a specific person's presence could reasonably be anticipated,
- apparent triggering event,
- admissions of intent or other communications by the subject reported before, during, and/or after the incident, and
- the nature of the subject's relationship with the victim(s) prior to the attack.

### *Targeting: Specifically Named Individuals*

In nearly three-quarters of the incidents (73 percent,  $n = 198$ ), subjects targeted one or more specifically named individuals. From context, their target selections appeared closely related to triggering events (e.g., romantic breakup, an academic or workplace failure, or a dispute), and, more often than not, were limited to the person or persons whom the subject may have blamed for causing the event. In a small fraction of these cases (2 percent,  $n = 6$ ), there was also some indication that the subjects intended to harm one or more random persons beyond the individuals they blamed. An example of the latter situation includes the following incident:

*On April 17, 1981, upset over failing grades and a possible second academic dismissal from the IHE, a 22-year-old student tossed a firebomb into the hallway of a dormitory and opened fire with a sawed-off shotgun as the occupants evacuated. Two students were killed. When police searched the subject's room, they found a gas mask, a second gun, and more than 100 shotgun shells as well as a notepad containing the name of one of the victims in the case. According to reports, this led police to believe that among the subject's random targets, there was at least one specific target whom the subject intended to harm.*

In over three-quarters of the incidents where specific individuals were targeted, these individuals were the only ones harmed (79 percent,  $n = 156$ ). In the remaining cases ( $n = 42$ ), the casualties



included collateral victims<sup>33</sup> and/or victims of opportunity.<sup>34</sup> Examples of variations among these types of cases include:

*Specific Individual Targeted and Additional Collateral Victim Harmed During the Incident:*

*On April 5, 1975, upset over failing his oral exam, a 25-year-old doctoral candidate shot and wounded an assistant professor from the review committee. The victim was sitting in a classroom with others who were waiting for a lecture to begin. Also wounded was a student bystander who came into the line of fire when he stood at the same time as the intended target. Reportedly, the subject had threatened the professor two days prior and a pistol was taken from him by campus police; however, he was not taken into custody at that time.*

*Specific Individual Targeted and Victim of Opportunity Killed During the Incident:*

*On December 17, 1983, at 11:30 p.m. on Saturday night, a 26-year-old subject who was not affiliated with the affected IHE, arrived at a dormitory to see his former girlfriend, a student, with whom he had become obsessed. When he arrived at her room, she reluctantly agreed to see him. When it became tense, the subject held the girlfriend, her roommate, and five others hostage using a silenced rifle. After the former girlfriend convinced him to release all but herself and her roommate, the subject fatally shot them both. He then drove off and shot himself in the head, but survived the wound.*

*Targeting: Random Individuals*

In approximately one-fifth of the incidents (21 percent,  $n = 58$ ), the subject's targeting appeared to be directed toward a single random individual or multiple random individuals. Examples of this type of targeting include the following:

*Random Individual Targeted:*

*On May 17, 2001, a 55-year-old subject who was not affiliated with the affected IHE, fatally shot an assistant music professor on a walkway outside a dormitory. He then took his own life. According to a note left behind, the subject chose the victim at random. He had become obsessed with another professor on that campus whom he had dated briefly in 1966. Though he had had no contact with her for nearly three decades, in 1995 he began stalking her. Frustrated at being rebuffed, he decided to kill himself and take someone else with him. He hoped that person would be someone known to her. In the note he left, the subject wrote, "I considered multiple murder but realized it's pointless. I finally decided to murder just one person. Just one is sufficient to teach a lesson."*

*Multiple Random Individuals Targeted:*

*On September 26, 1977, distraught over pressures to perform from his parents, a 22-year-old student fatally shot his apartment manager, then grabbed a rifle and one of his handguns and went to the campus. He entered a typing lab in the Business Administration Building, then, in front of 30-40 students, fired off a few shots. One shot struck a teacher's aide. He then sought one of the fleeing*

---

<sup>33</sup> "Collateral Victim" is defined as a person who was injured or killed during the execution of the attack and (a) was not specifically selected or contemplated in advance, and (b) whose actual harm was incidental during the execution of the attack.

<sup>34</sup> "Victim of Opportunity" is defined as a person who was injured or killed during the execution of the attack and (a) was not specifically selected or contemplated in advance, but (b) whose selection as an appropriate object of harm, consistent with the subject's apparent motive or goals, was made at the time of the incident.

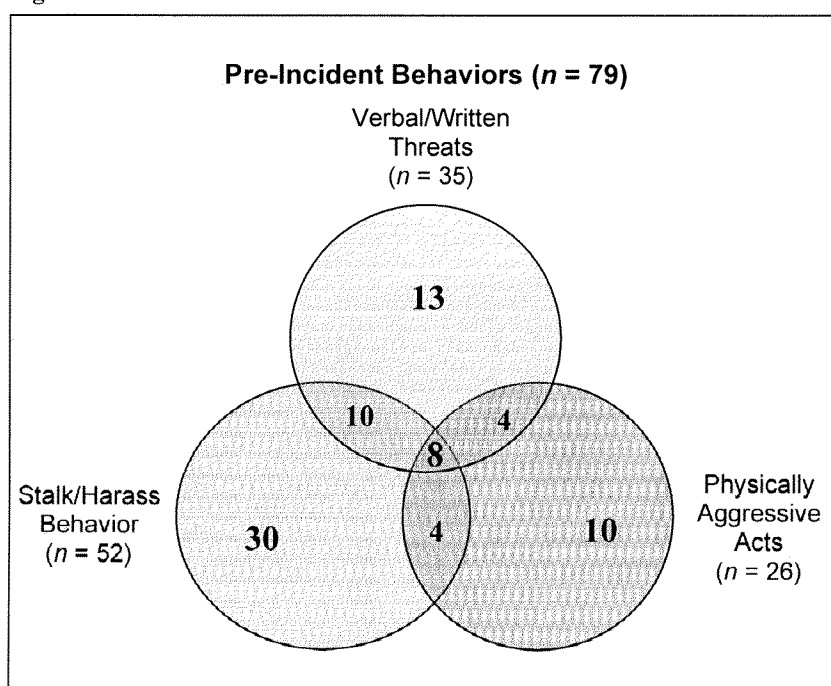


students, placed the rifle to her head, and pulled the trigger, however the rifle jammed. He then went to another classroom and fatally shot himself.

### ***What pre-incident behaviors were directed toward the targets?***

Though information on the subjects' behaviors prior to the incidents was not always reported, efforts were made to identify whether the subjects engaged in verbal and/or written threats, stalking or harassing behaviors, and/or physically aggressive acts directed toward the targets prior to the incidents. In 29 percent ( $n = 79$ ) of the incidents, subjects engaged in one or more of these actions directed toward the target. Figure 4 illustrates how these behaviors overlapped.

**Figure 4**



#### ***Verbal/Written Threats***

In 35 incidents (13 percent), open-sources reported that the subjects made verbal and/or written threats to cause harm to the target. These threats were both veiled and direct, and were conveyed to the target or to a third party about the target. An example includes:

*On April 12, 1982, a 28-year-old former student entered the office of a psychology professor and fatally shot him before eight witnesses. According to investigators, the victim was warned several times about the subject's threats on his life. IHE officials reported that the week prior to the attack, they had received a call from a psychiatrist who said he was treating a man who once took the victim's class and now wanted to kill the professor. The victim reportedly had discussed the threats with students during classroom lectures on fear.*



### *Stalking/Harassment*

Open-sources reported stalking or harassing behavior in 52 incidents (19 percent). These behaviors occurred within the context of a current or former romantic relationship or in academic and other non-romantic settings. They took on various forms, including written communications (conventional and electronic), telephonic contact, and harassment of the target and/or the target's friends/family. Subjects also followed, visited, or damaged property belonging to target(s) or their families prior to the attack. Examples include the following incidents:

*On July 25, 1989, a 24-year-old subject who was not affiliated with the affected IHE, tracked down his former girlfriend who had moved to another state to avoid him, and confronted her in the IHE parking lot as she walked with a male friend. When she would not go with the subject, he shot and killed them both. The subject had hired a private detective agency to track her down and was able to obtain information on the victim through bank records and the IHE registrar.*

*On April 10, 1996, upset over losing his friendship with the victim, a 19-year-old student confronted his former friend on campus, fatally shot him in the back of the head, flipped him over with his foot and fired another shot into his chest. Months prior to the incident, the victim reported to IHE administrators that the subject had been harassing him by sending e-mails and calling numerous times. The subject, who had completed his degree requirements in December 1995, was told by administrators to stay away from the campus. On the day of the incident, in accordance with an agreement he made with the IHE, the subject had informed the dean of his intended presence on campus that day. The subject had completed his degree requirements and was awaiting graduation.*

### *Physically Aggressive Acts*

Open-sources reported that subjects engaged in physically aggressive acts toward the targets in 26 incidents (10 percent). These behaviors took the form of physical assaults, menacing actions with weapons, or repeated physical violence to intimate partners. An example includes:

*On August 12, 1996, upset over his girlfriend (student) breaking up with him 10 days prior, a 27-year-old subject (not affiliated with the IHE) arranged to meet her on campus. Once there, he fatally shot her in the parking lot, then himself. Witnesses described that the subject had been physically and mentally abusive toward the victim during their one-year relationship. Just four months before this attack, the subject held a 13-inch blade to the victim's throat, tying her hands with a scarf, and threatening to kill her.*

### ***Did others observe concerning behaviors just prior to the incidents?***

Information on whether the subjects engaged in concerning pre-incident behaviors was not always reported. Open-sources may report their presence, but rarely confirm their absence. With this in mind, attempts were made to explore any discernable behaviors that may have occurred just prior to the incidents and warranted concern by those surrounding the subjects. The behaviors noted are purely descriptive and should not be considered comparative or predictive.



Concerning behaviors were observed by friends, family, associates, professors, or law enforcement in 85 incidents (31 percent).<sup>35</sup> These behaviors included, but were not limited to: paranoid ideas, delusional statements, changes in personality or performance, disciplinary problems on campus, depressed mood, suicidal ideation, non-specific threats of violence, increased isolation, "odd" or "bizarre" behavior, and interest in or acquisition of weapons. Examples include the following:

*On May 19, 1936, possibly upset over academic pressures, a 19-year-old freshman fatally shot one student and wounded another as the students entered his dorm room. He then killed himself. He had reportedly purchased two guns from a mail order house a few days earlier. When this was discovered, the subject was ordered to turn the weapons over to the dean, which he promised a student adviser he would do. The subject's father also stated his son's recent letters had been "strange and hard to understand." A classmate stated that the subject had been "telling us fellows for a week that he had been planning suicide."*

*On January 26, 1992, a 22-year-old campus police officer pulled over a nursing student whom he did not know, drove her to a deserted campus parking lot, removed her clothing and shot her 14 times. Prior to the incident, the subject was linked to other crimes, which were known to the IHE. He was suspected in a series of campus fires, firing a bullet through a dormitory window, inventing a break-in, calling a suspect at home, and phoning in a bomb threat.*

In 29 percent ( $n = 25$ ) of the incidents involving concerning behaviors, the offenders also exhibited one or more acts involving stalking/harassment, written/verbal threats, or physically aggressive acts toward the target.

In those cases in which concerning behaviors were not observed ( $n = 187$ ), media reports described other significant criminal, violent, or mental health histories unrelated to the incident ( $n = 14$ , 8 percent). This included multiple criminal or violent acts, a series of psychiatric hospitalizations, and/or the presence of psychotic symptoms over an extended period of time. An example is:

*On January 12, 1980, the 24-year-old student manager of the tennis team fatally stabbed a campus tennis star outside of the dorm. During trial it was revealed that the subject had been expelled from six schools due to behavior problems, saw at least a dozen mental health professionals, and spent time in at least six hospitals. In addition, witnesses described specific violent incidents, such as hitting a neighbor's son with a hammer, setting fire to his house, attacking a stranger on a train platform, and striking a co-worker over the head with a metal pipe.*

---

<sup>35</sup> It should be noted that those persons who reported the concerning behaviors were not necessarily trained in the recognition of psychiatric or psychological symptoms.



## CONSIDERATIONS

Campus threat assessment teams that seek to employ reasoned and effective risk mitigation strategies may recognize the potential significance of findings presented in this preliminary report.<sup>36</sup>

### *General Observations*

Several general observations concerning the data have relevance to the domain of threat assessment and threat management.

- Incidents of targeted violence are a year-round issue. Campus safety resources may be required throughout the calendar year, not just during the academic year.
- On-campus targeted violence is not the only challenge, as 20 percent of the incidents took place off-campus or in non-campus IHE locations against targeted IHE members. This suggests that communication between campus safety professionals and municipal law enforcement agencies is essential.
- Of those incidents that occurred at on-campus or non-campus sites ( $n = 217$ ), 36 percent took place in administrative/academic/services buildings, 28 percent took place in residential buildings, and 27 percent took place in parking lots or campus grounds. On-campus mitigation plans should equally cover responses to IHE buildings, IHE operated residences, and IHE parking lots and grounds.
- Only 3 percent of on/non-campus attackers ( $n = 217$ ) moved *between* buildings. Of those that were carried out *within* the same building ( $n = 159$ ), only 4 percent of the attackers moved to different locales (e.g., classrooms, offices, hallways). Though much attention has been given to the phenomenon of the “traveling” attacker, in context, it actually is a rare event. This finding may have tactical and strategic ramifications for first responders and emergency management professionals.
- Firearms and knives/bladed weapons were used most frequently (75 percent) during the incidents. The remaining 25 percent of the incidents involved strangulation, blunt objects, poison, vehicles, explosives, incendiary/arson methods, or physical assaults without a weapon. Understanding the varied weapons used in these incidents may prompt investigators to look beyond whether a subject possesses or has access to a more traditional weapon (firearm or knife) when evaluating his or her risk.

---

<sup>36</sup> Before implementing a threat assessment model, IHEs should consult with legal counsel as they develop their threat assessment process, policies, and protocols. Specifically, legal counsel should be asked to review and consider relevant federal and state statutes about information sharing, e.g., the *Family Education Rights and Privacy Act (FERPA)*, as well as those concerning an IHE’s civil rights obligations (e.g., the *Civil Rights Act of 1964* and the *Rehabilitation Act of 1973*). More information can be found at: <http://www2.ed.gov/about/offices/list/ocr/index.html>.



### ***Diversity of the Subject Population***

A great deal of concern is given to conducting threat assessments of current students who may pose a threat of targeted violence. This level of concern is not entirely misplaced as current students represented 45 percent ( $n = 121$ ) of the subjects in those incidents in which the subjects' affiliations were identified ( $n = 268$ ). The violence documented in the remaining 55 percent of the cases included former students (15 percent), current and former employees (11 percent), subjects indirectly affiliated with the IHE (20 percent), and subjects with no known affiliation with the IHE (9 percent). The unique and open nature of most universities necessitates acknowledgement of the many diverse threats to campus safety. It is clear that focusing solely on the student attacker as a potential threat to campus safety ignores the fact that many IHEs are workplaces, residences, and communities that routinely host a wide range of activities that attract a variety of individuals, many of whom do not have any direct relationship to the college or university.

From a threat assessment perspective, the fact that 30 percent of the subjects were either unaffiliated or indirectly affiliated with the IHE through students or employees, three-quarters of whom were current or former spouses or intimate partners, challenges campus and law enforcement personnel to design a threat assessment capability that can also identify and assess threats that go beyond their student and employee populations. By establishing connections to community resources ahead of time, campus safety professionals may enhance their ability to prevent a threat from materializing that originated from an indirectly affiliated subject.

Additionally, although the average subject age was 28 ( $n = 260$ ,  $Mdn = 25$ ,  $mode = 20$ ), these preliminary findings highlight the wide range of offenders' ages (16 to 62) and suggest the need for a flexible analysis and response protocol. As developmental issues and situational stressors change across a lifespan, standard practices should incorporate multidimensional risk factors germane to specific stages, from adolescence to mature adulthood. Similarly, IHEs traditionally host multi-ethnic, culturally diverse populations, further requiring contextually appropriate considerations. While this phase of the project did not address the ethnic backgrounds of the subjects, it is anticipated that the Department of Education and the FBI, in the next stages of this research, will highlight the need for IHE threat assessment teams to recognize and assess behaviors exhibited by a pool of individuals representing a broad range of ages, cultures, past life experiences, and current situational contexts.

### ***Diversity of Criminal and Other Concerning Behaviors***

IHE campuses essentially function as mini-societies that must deal with the same types of societal issues found in almost any city or town in the United States. Whether the setting is a more traditional campus with distinct boundaries, an urban campus that is interlaced within a larger community, or somewhere in between, most campuses must contend with their own social norms, economy and culture. IHEs must then establish an infrastructure capable of providing the necessary services, support and protection to students, staff, and others who may have contact with the IHE. Looking at the protection side alone, as a mini-society, IHEs must contend with the full range of crimes committed by or against its members.



All forms of targeted violence were found among the incidents. The identified incidents dealt with domestic violence, workplace violence, stalking and obsessions, sexual assaults resulting in homicide, individualistic stressors, subjects acting on delusional beliefs, as well as serial killers. Because of this diversity of crime, those responsible for threat assessment may need to build a program that is flexible and comprehensive enough to address all aspects of targeted violence. This may require university threat assessment teams to employ a wider breadth of resources that will educate and support them as they address the full range of targeted violence.



## CONCLUSION

For this paper, researchers relied on open-source information to capture the nature and magnitude of violence affecting America's colleges and universities. Therefore, the observations and recommendations are necessarily limited, and readers should be cautious to avoid drawing broad-based conclusions. What is offered here, then, is not the end of the process, but a preliminary look at the scope of this issue. Several of the key elements explored included the attackers' intent with regard to target selection, interpersonal relationships, personal stressors, and triggering events. Each of these elements seemingly played a significant role in the offenders' decision to commit an act of violence. In nearly three-quarters of the captured incidents, the offender appeared to have targeted one or more specifically named individuals. Only in a small percentage of the cases was there some indication that random persons were also targeted along with specific individuals. Hence, understanding what leads an offender to exclusively target random individuals remains a complex and difficult challenge.

For years, colleges and universities have worked to address this challenge—to create safe campuses where academic and personal growth can flourish. In the wake of the Virginia Tech tragedy, many universities were confronted with the troubling reality that one person can, in a few brief moments, devastate a college community through an act of targeted violence. In the effort to thwart such individuals, IHEs have created threat assessment teams. These teams typically comprise representatives from various departments within the college or university, including academic affairs, student affairs, the IHE's general legal counsel, mental health services, and public safety. IHE threat assessment teams seek to thoroughly evaluate persons of concern who may pose a potential risk of violence and generally engage in a three-step process:

- Identify individuals, whose behavior causes concern or disruption on or off campus, affecting IHE members such as students, faculty, or other staff.
- Assess whether the identified individual possesses the intent and ability to carry out an attack against the IHE or members of the IHE community, and if the individual has taken any steps to prepare for the attack.
- Manage the threat posed by the individual, to include disrupting potential plans of attack, mitigating the risk, and implementing strategies to facilitate long-term resolution.

IHE threat assessment teams that perform this important function are routinely faced with several key issues during each evaluation: identifying the specific behaviors that are suggestive of an attack against persons affiliated with an IHE (including students, faculty, and staff); considering whether concerning, suicidal, or threatening behaviors are warning signs of a violent act; and fostering a secure environment while simultaneously promoting academic freedom and creative expression, and protecting student privacy.<sup>37</sup>

---

<sup>37</sup> The threat assessment process is based on the premise that each situation should be viewed and assessed individually and guided by the facts. Judgments about an individual's risk of violence should be based upon an analysis of his/her behaviors and the context in which they occur. Blanket characterizations, demographic profiles, or stereotypes do not provide a reliable basis for making judgments of the threat posed by a particular individual.



With these challenges in mind, the participating agencies in this study have collaborated in an effort to further understand targeted violence at colleges and universities. The goal of this phase of research was to identify and examine incidents of targeted violence that have occurred at IHEs or against members of the IHE community. As the project enters into the next phase, the FBI and the Department of Education will thoroughly examine case files and investigative records from campus attacks in an effort to better serve the professionals who work to ensure campus safety. The next phase will include a more detailed examination of characteristics that were difficult or impossible to measure due to inadequate or missing information in the open-sources (e.g., mental illness, past behavior). The researchers are optimistic that by exploring violence against IHE students, faculty, and staff, some offenders can be identified prior to an attack and many lives can be saved.



## APPENDIX A: IHE Definitions

**IHE Campus/Facility:** IHE grounds (e.g., areas between buildings, landscaped areas), parking lots, buildings (e.g., classroom buildings, dining halls, student unions, research centers, dormitories, fraternity/sorority houses, other university-sponsored student housing), and built venues (e.g., stadiums) that are owned, leased, operated, or reserved by the IHE for permanent or temporary use.

**IHE Employee:** Member of an IHE's faculty, staff (e.g., mental health counselors, building maintenance personnel, campus law enforcement, financial aid counselors, medical personnel), or administration (e.g., dean, president, provost, vice president), an IHE contractor, or an individual employed by an IHE contractor.

**IHE Event:** IHE sporting, ceremonial (e.g., graduation, award dinners), entertainment, and educational activities (e.g., student government meetings) sponsored or sanctioned by the IHE or an association affiliated with the IHE.

**IHE Student:** Individual enrolled in a college or university (e.g., undergraduate, graduate, full- and part-time). The student may still be enrolled at the IHE even though he or she is not registered for classes at the time of the incident.

**Non-Campus:** "Any building or property owned or controlled by a student organization that is officially recognized by the institution; or Any building or property owned or controlled by an institution that is used in direct support of, or in relation to, the institution's educational purposes, is frequently used by students, and is not within the same reasonably contiguous geographic area of the institution."<sup>38</sup> Examples include research facilities, university-owned hospitals, off-campus student housing facility owned by a third party that has a written contract with the institution to provide student housing, student residential facility owned or controlled by the institution, a publicly owned athletic stadium that is leased by the institution for its football games.

**Off-Campus:** All other buildings or facilities that may be used by IHE students or IHE employees for housing and/or recreation but are not officially associated with an IHE. Examples include privately leased apartments, privately owned residences, social clubs, or restaurants.

**On-Campus:** "Any building or property owned or controlled by an institution within the same reasonably contiguous geographic area and used by the institution in direct support of, or in a manner related to, the institution's educational purposes, including residence halls."<sup>39</sup> Sorority or fraternity houses that are located within the same reasonably contiguous geographic area of the institution are included as on-campus, even if they are not controlled or owned by the IHE.

---

<sup>38</sup> *Higher Education Act*, 34 C.F.R. 668.46(a).

<sup>39</sup> *Ibid.*



## **APPENDIX B: Additional Examples of Incidents**

### ***Subjects who moved from one location/building to another:***

On August 12, 1986, a 29-year-old student went on a shooting rampage on campus, injuring four and fatally shooting one. The subject had purchased two guns out of state the day before. When he returned, he went straight to the campus laboratory where he fatally shot one of his intended targets, a lab technician with whom he had worked. He then ran to the campus financial aid office in a second building, where he shot and wounded three more people, including the financial aid director who was another intended target. After firing shots at campus officers behind the second building, he raced into a third building, where he shot and wounded a security officer. After being cornered on a stairwell, he eventually surrendered to police. The attack appeared to be related to a dispute over \$717 in financial aid. He reportedly was due to receive the funds beginning the next month.

On November 1, 1991, a 28-year-old former student opened fire in two different buildings on campus. The subject had received his doctoral degree the previous May. Months before the shooting, he wrote five letters explaining the reasons for his planned actions. Intended for news organizations, they stated that he was angry and jealous that his doctoral dissertation had not received a prestigious academic award and he was upset over perceived mistreatment and his inability to find work. The subject allegedly had specific targets that included his academic advisor, the chairman of his department, an assistant professor and his former roommate. After fatally shooting them in his department building, he then walked three blocks to another building and asked to see the assistant vice president for academic affairs. After fatally shooting her, he turned and wounded the student assistant seated there. He eventually fatally shot himself.

On March 24, 1999, a 25-year-old former student fired a gun in the Agricultural Building on campus, striking a door. The shot just missed two female students in the hallway by a few inches. Approximately 20 minutes later, the subject fired another shot at a student sitting in a courtyard on the same campus, striking the student in the left arm. Though media reports did not reveal a motive for the attacks, they did connect him to another shooting on another campus the following day. In that incident, the subject fired a shot in the hallway of a new academic building on a campus with which he had no known affiliation. The shot grazed the side of a female who was on campus visiting her father, a professor on that campus.

### ***Subjects who moved between multiple locales within the same building:***

On April 25, 1950, a 54-year-old professor went to the second floor office of the college president, fatally shooting him. He then went downstairs to the office department chair, the subject's immediate supervisor, and fatally shot him. The subject then returned home and killed himself. Investigators found the body and several notes. Reportedly, the subject suspected he would be fired but had not been officially informed. When the new college catalogue was issued on the morning of the incident, the subject saw that his name was not included after 24 years with the college.



On November 11, 1971, a 21-year-old non-affiliated subject entered a campus church with a rifle, pick ax, and a sledgehammer. When he encountered the caretaker, the subject fatally shot him in the back. He then used the sledgehammer to smash statues, pews, and windows. He then ran outside, randomly firing at passersby, injuring four. He was later killed by police at the scene. Following the shooting, the subject's father blamed LSD, stating that his son had become a religious fanatic, convinced that "Christ was an imposter."

On October 6, 1979, shortly after midnight, a 19-year-old student opened fire at a crowded fraternity party in a dorm, shooting five students. He then ran outside and shot two more students. In total, five students were injured, two were killed. His defense attorney blamed a "second personality" and brain damage from a car wreck as a child. The prosecutors stated that the subject had attended one of the fraternity's parties two weeks prior and was mad that his two-dollar cover charge was not refunded after police broke it up.

On May 4, 1983, a former employee (age not reported) entered a campus library, shot and wounded the director of libraries in his office. He then walked into an adjacent conference room with 20 people inside and fired two shots at his former supervisor, missing both times. After reloading his weapon in a restroom, he left the floor and headed to the main desk. Once there, he unloaded his weapon, put it down and waited for police. The subject had been fired from the library just three months prior after 19 years of service.

On January 16, 2002, a 43-year-old former student went to the offices of the college dean and a professor, fatally shooting them both. He then descended a stairway into a common area and opened fire on a crowd of students, killing one and wounding three others. Days before the shooting, faculty had informed the subject that they were dismissing him from the school due to his failing grades. Police said the shooting occurred after he arrived to protest his dismissal.

On May 9, 2003, at 4 p.m., a 62-year-old former student, who had also been employed by the IHE in the past, opened fire on the exterior of the business school building on campus. He then used a sledgehammer to smash his way through the entry. He reportedly fired hundreds of rounds of ammunition while he wandered the halls of the building. One student was fatally shot, while a professor and student were wounded. The subject was reportedly looking for a computer lab technician whom the subject had sued for hacking into his Web site and he wanted to punish the university for protecting him. The attack ended about 11 p.m. when officers shot and wounded the subject.

***Subjects who carried out multiple attacks on the same campus within 1-2 months:***

Starting in February 1982, four separate shootings took place on a college campus and were committed by a 32-year-old former student, later identified as a neo-Nazi serial killer. On February 1, the subject fatally shot a popular local pastor in a men's room in a classroom building on campus. Later, on August 9 and August 27, he shot at two employees also in restrooms located on campus, missing one and killing the other. Three days later, he fatally shot a 17-year-old student enrolled in a high school equivalency program at a bus stop in front of the campus. The subject was also connected to another sniper-style attack that took place off-campus



at a train station that June. The victim wounded in that attack was not affiliated with the affected IHE.

On August 31 and September 22, 1999, a 41-year-old unemployed funeral embalmer and father of two set off two pipe bombs in restrooms in administrative and classroom buildings on campus. Both explosions were accompanied within minutes by racist phone calls to a local TV station, and the last one included a warning that the two blasts were "just the beginning." Though there was only minimal damage with no injuries, 400 students withdrew from the university in the aftermath. The subject was a former vending company employee who once had a delivery route at the campus and had serviced machines in the two buildings where the bombs were detonated. He also held a university-issued ID card for this job, and a former coworker told investigators he did not return it when he left the company in July 1999.

***Examples of stalking or harassing behaviors exhibited by subjects prior to the incidents:***

***Acquaintance Harassment:***

On November 29, 1992, a box of candy was received by a 26-year-old female student. The student did not eat the candy; rather, she turned it over to police. According to the authorities, the candy was spiked with thallium. The unmarked package was traced to a former student who had studied at the IHE from August 1990 to May 1991. The target had rejected the subject's romantic advances and leveled verified charges of harassment against him, causing him to be removed from the IHE. The subject had sent a similar package to another female student in another state. In that case, the victim consumed the candy as did her roommates. The victim and three others were hospitalized. After the subject was identified, it was revealed that he had a history of stalking the second victim in their native country of Belgium.

***Stranger-Based Stalking:***

On January 13, 1998, a 27-year-old subject, not affiliated with the affected IHE, killed an IHE campus police officer after striking him more than 20 times with a hatchet. The officer had been sitting in his squad car doing paperwork at the time. Witnesses would later testify that the subject stalked the victim prior to the incident and repeatedly informed family and friends that he wanted to kill a cop.

***Academic-Based Harassment:***

On August 24, 2006, upset over his dismissal from a master's degree program, a 25-year-old former graduate student set four small fires at a professor's home. The professor and his two teenage children escaped the home without injury and the fires were extinguished with minimal damage to the home. The subject was later captured in a wooded area nearby where he had tried to kill himself with a drug overdose. In October 2005, the victim had filed a complaint with the police department that the subject was making harassing phone calls to his home. Additionally, the subject had sent e-mails to his internship supervisor that were sufficiently "aggressive" in tone that a police officer was stationed outside her classroom for the last three classes the subject attended.



## APPENDIX C: Definitions of Incident Categories

**Acquaintance/Stranger-Based Sexual Violence**—Directed assaults that included sexual violence between persons known or not known to each other, excluding those subjects and targets who were current or former intimates.

**Bias Related**—Directed assaults in which the subject appeared to be motivated by a bias against the target based on race/ethnicity, religion, or other characteristics.

**Draw Attention to Self/Issue(s)**—Directed assaults in which the subject's actions were intended to draw attention to the subject, the subject's actions, or a specific issue other than one based on bias.

**Need to Kill/Specific Victimology**—Directed assaults in which the subject appears to be motivated by a general need to kill or selection of a target that matches a victim profile (a set of demographic or other perceived static traits that the subject(s) sought in selecting a target).

**Psychotic Actions**<sup>40</sup>—Directed assaults where the subject's actions appeared to be as a result of delusions, paranoia or hallucinations.

**Refused Advances or Obsession with the Target**—Directed assaults in which the subject's actions appeared to be a response to romantic or interpersonal rejection and there was no clear indication that the subject and the target had an intimate relationship. This also includes a subject who was obsessed with a target, of which the target was never aware.

**Related to an Intimate Relationship**—Directed assaults in which the subject retaliated against a current or former intimate partner (e.g., husband, wife, boyfriend, girlfriend) for any reason (e.g., breakup, divorce, affair, filing court papers). This could also include retaliation against a proxy for that intimate partner (e.g., the current partner, or mistress).

**Response to Academic Stress/Failure**—Directed assaults in which the subject's actions appeared to be the products of academic stress, rejection or failure.

**Retaliation for Specific Action(s)**—Directed assaults in which the subject's actions were in retaliation for a specific act (including statements) committed by or perceived to be committed by the target, but that does not meet the definition of the other options. The retaliatory attack could be directed toward a third party.

**Undetermined**—Open-source did not contain enough information to determine one clear motive or trigger for these incidents.

**Workplace Dismissal/Sanction**—Directed assaults in which the subject appeared to be responding to an impending or actual dismissal/suspension or forced resignation, or was retaliating for a past or present workplace legal action or other difficulty.

---

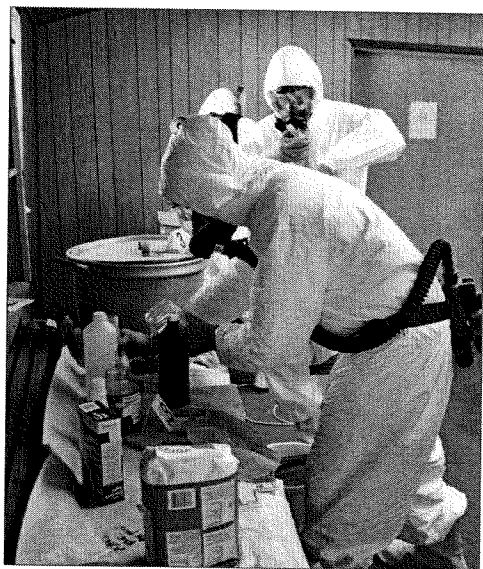
<sup>40</sup> For a discussion on "psychotic action" see Junginger, J. (1996). Psychosis and Violence: The Case for a Content Analysis of Psychotic Experience. *Schizophrenia Bulletin*, 22 (1), 91-103.



## Science and the FBI

The FBI recognizes the importance of scientific progress, as well as the development and peaceful dissemination of technology. We work hard to ensure our efforts do not impede scientific research. It is our intent, in partnership with the scientific and academic community, to help protect the United States.

Mutually beneficial relationships require open lines of communication to ensure understanding and to identify opportunities for collaboration. The FBI has WMD Coordinators located in all 56 field offices across the United States. Your WMD Coordinator will help you become more aware of potential chemical WMD threats and develop a plan with you to report suspicious activities. We hope to benefit from your knowledge of emerging trends and technologies to prevent a chemical attack.



## How Can I Help?

- Distribute FBI materials to help faculty, students, and lab personnel increase their awareness of chemical terrorism.
- Help the FBI identify possible vulnerabilities within the chemical academic sector.
- Encourage open discussion about potential chemical threats and report suspicious behavior or events to your local FBI WMD Coordinator.

## For More Information

FBI offices are located in major cities throughout the United States, San Juan, Puerto Rico, and abroad. In addition, resident agencies are maintained in smaller cities and towns across the country. The FBI encourages the public to report any suspicious activity and suspected violations of the US Federal law. You can do so by calling your local FBI office, Legal Attaché (LEGAT) office, or by submitting a tip via the FBI Tips and Public Leads at [www.fbi.gov](http://www.fbi.gov)

Telephone: 202.324.3777

E-mail: [chemteam@fbi.gov](mailto:chemteam@fbi.gov)

Website: <http://www.fbi.gov/about-us/investigate/terrorism/wmd>

Federal Bureau of Investigation  
Weapons of Mass  
Destruction Directorate

# Academic Chemical Security





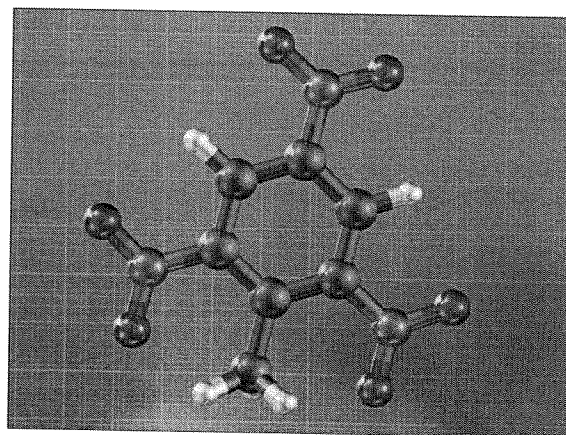
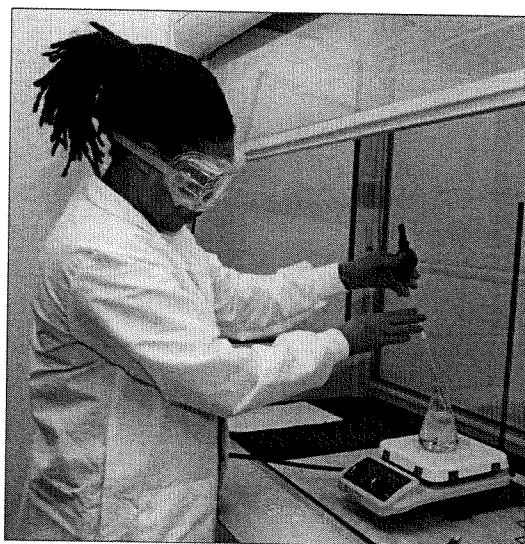


## Why Outreach?

Many extremist individuals and terrorist groups have expressed the intent to attack the United States using chemical weapons and improvised explosives. University laboratories, various Internet sources, chemical suppliers, and retail stores that house or sell chemical precursors are potential sources of information, skills, tools, and materials required to carry out such an attack.

Faculty, students, researchers, and laboratory personnel need to be aware of these threats and understand the warning signs of being targets for the exploitation of knowledge, skills, or acquisition of tools or materials needed to make a weapon of mass destruction (WMD). Awareness of suspicious behavior indicators can lead to early detection of nefarious activity.

The FBI's Chemical Academic Outreach Program is designed to educate faculty, students, and staff about the FBI's WMD mission, its capabilities, and its chemical counterterrorism initiatives.



## Chemical Threats

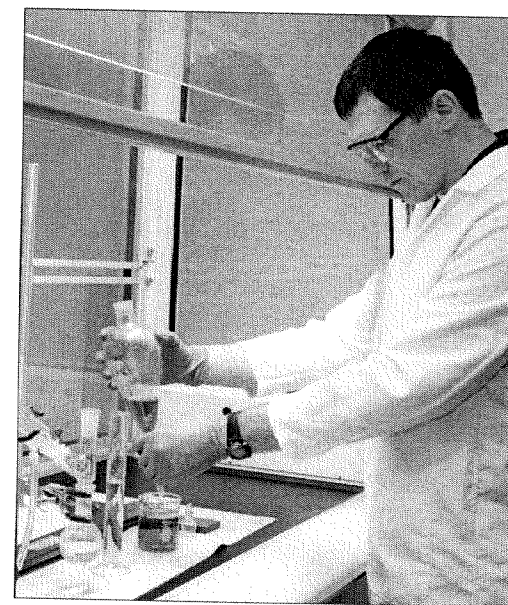
A chemical attack is the deliberate use of chemical materials such as toxic industrial chemicals, chemical warfare agents, and improvised explosives that can be used to harm people, plants, animals, and our country's critical infrastructure. Individuals who intend to carry out attacks using a chemical or improvised explosive device need to know what you and your colleagues already know:

- how to acquire chemicals and glassware
- how to handle chemicals safely
- how to follow chemical synthesis procedures
- how to purify and disseminate the resulting chemical agent

Individuals may contact you to obtain technical chemical information through e-mail and online chat rooms, or they may approach you at conferences to ask seemingly innocent questions about your research. While most of these questions will be legitimate or innocent, there is a risk some are not and may indicate a potential threat. Other indicators of potential threats include suspicious behavior in the laboratory or missing supplies and chemicals.

## What Should I Be Aware of?

- Individuals attempting to access the laboratory who generally have no reason to be there
- Missing supplies, chemicals or lost or moved laboratory equipment
- Requests to borrow chemicals or equipment from unidentified individuals
- Unsolicited requests for technical information in person or over the Internet
- Unusual employment or collaboration requests
- Chemical purchases charged to a lab purchase card or grant but are never delivered
- Unsolicited delivery of chemicals to the lab without a corresponding chemical purchase





FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1212788-0

Total Deleted Page(s) = 11  
Page 25 ~ b6; b7C; b7E;  
Page 26 ~ b7E;  
Page 27 ~ b7E;  
Page 175 ~ Referral/Consult;  
Page 181 ~ b6; b7C;  
Page 183 ~ b6; b7C; b7E;  
Page 184 ~ b6; b7C; b7E;  
Page 205 ~ b7E;  
Page 218 ~ b6; b7C; b7E;  
Page 219 ~ b6; b7C; b7E;  
Page 224 ~ b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX



~~SECRET~~

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

[REDACTED] RMD)(CON)

From: [REDACTED] SE) (FBI)  
Sent: Monday, November 10, 2014 6:42 PM  
To: [REDACTED] (RMD)(CON)  
Subject: [REDACTED] ~~SECRET//NOFORN~~

b6  
b7C  
b7E

Follow Up Flag: Follow up  
Flag Status: Flagged

SentinelCaseId: TRANSITORY RECORD

Classification: ~~SECRET//NOFORN~~

ATTORNEY WORK PRODUCT/ATTORNEY-CLIENT PRIVILEGED INFORMATION/DELIBERATIVE  
PROCESS PRIVILEGED DOCUMENT

Upon removal of attachment(s), this document is UNCLASSIFIED//~~FOUO~~

~~Classified By: C67W98B51~~  
~~Derived From: FBI NSIC, dated 20120629~~  
~~Declassify On: 20391231~~

=====  
TRANSITORY RECORD

Good afternoon [REDACTED]

b5  
b6  
b7C

Take Care,  
[REDACTED]

~~SECRET~~

(S) [REDACTED]  
[REDACTED] UI progr...

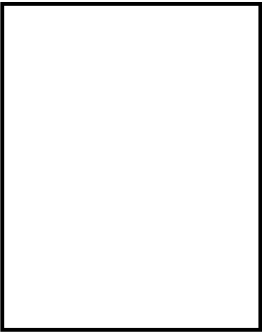
b1  
b3

[REDACTED]  
~~SECRET//NOFORN~~

b5

~~SECRET~~





b5



Supervisory Special Agent  
Chief Division Counsel  
Seattle

b6  
b7C



main  
direct

\*\*\*\*\*

Classification: ~~SECRET//NOFORN~~



[REDACTED] (RMD)(CON)

**From:** [REDACTED] (CTD) (FBI)  
**Sent:** Wednesday, February 26, 2014 2:05 PM  
**To:** [REDACTED]  
**Subject:** FW: Brief Active Shooter update --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

**From:** [REDACTED] (DM) (FBI)  
**Sent:** Wednesday, February 26, 2014 1:56 PM  
**To:** [REDACTED]  
**Subject:** Brief Active Shooter update --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

Good afternoon from the Active Shooter Team,

Three short items I ask you to please share with your Division personnel as appropriate.

1. Active Shooter Initiative Lead SC Christopher H. Combs has been named SAC San Antonio and therefore will be leaving the team. Chris has been the heart and soul of this effort from the day the Deputy Director asked him to take on this project. His insight and forward-leading views have led the team as FBIHQ and the field have marked substantial accomplishments this past year. We will miss his dedication, knowledge and tenacity, as will our White House working group members. We wish him well in San Antonio.

2. InfraGard in FBIHQ has put into Bu-mail the pocket Active Shooter Quick Reference Guides as interest continues to grow for information from businesses and schools; the groups most involved in active shooter events. We ask your active shooters speakers to support speaking requests from InfraGard using the Active Shooter Public Awareness presentation located on the CIRG Active Shooter resources page noted here:

[REDACTED] This presentation also is available for Citizens Academy and other community outreach presentations.

b7E

3. Conferences and TTXs - Interest from FBIHQ remains strong that field offices continue to engage with state, local, tribal and campus law enforcement, as well as first responders, to share best practices and lessons learned about active shooter events. Criticism levied on the conferences primarily focus on unprepared speakers. If your office does not have a strong speaker for a particular part of the conference schedule, please reach back to FBIHQ to see if someone is available. The active shooter team is in the middle of a comprehensive analysis of these events, which should provide more insight during the next year into such incidents. Some field office personnel have asked whether we still have travel money for FBI and non-FBI employees. The answer is **YES**. Please follow the instruction in the EC, which includes TR#s.

[REDACTED] If you are using a TR#, you must also email their names to me and [REDACTED] from CIRG finance. I must provide email authorization to utilize the TR# for the traveler which must be attached this authorization to their TRIP request. CIRG FMU [REDACTED] must also be notified so that she can sub-allocate the funding to the office of the traveler. Therefore, can you please make sure you email me with the information on travelers and use of the TR# in addition to the EC required.

b6  
b7C  
b7E



Thanks [redacted]

UC [redacted]

Active Shooter Initiative

[redacted]

b6  
b7C

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



[REDACTED] RMD)(CON)

**From:** [REDACTED] SE)(FBI)  
**Sent:** Tuesday, February 04, 2014 1:16 PM  
**To:** [REDACTED] SE)(FBI)  
**Subject:** RE: Active Shooter question for the field, others can delete --- UNCLASSIFIED

b6  
b7C

Classification: UNCLASSIFIED  
=====

[REDACTED]

I am the Crisis Mgt Coordinator. [REDACTED] is the Training Coordinator. That being said, I have done all of the AS training; the initial TTX and seminar, followed by the Mall AS TTX. Do you think UW would be interested in a TTX? Although the MALL AS TTX was geared toward a Westgate type attack, the same principles apply for a stadium or any major venue. Also, I have some handouts that we can give the campus police they may find interesting (Crisis Communications for Commanders (media), Victim- Witness stuff, etc) Thx, [REDACTED]

b6  
b7C

**From:** [REDACTED] (SE) (FBI)  
**Sent:** Monday, February 03, 2014 11:00 AM  
**To:** [REDACTED] SE)(FBI)  
**Subject:** FW: Active Shooter question for the field, others can delete --- UNCLASSIFIED

Classification: UNCLASSIFIED  
=====

[REDACTED]

Are you SE's Active Shooter Coordinator?

Trying to get plugged in so HQ can see some documentation on our end from the CLI program.

b6  
b7C

Thanks

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Monday, February 03, 2014 4:01 AM  
**To:** [REDACTED]  
**Subject:** FW: Active Shooter question for the field, others can delete --- UNCLASSIFIED

b7E

Classification: UNCLASSIFIED  
=====

CLAs –

As you can see from the email below, your efforts to train campus public safety on Active Shooter events is recognized and appreciated at the highest levels. Of course, no good deed goes unpunished. You are now being requested to coordinate with your Training Coordinator and the Active Shooter Coordinator in your office to conduct more Active Shooter seminars for campus public safety in your AOR.

As requested in an email I sent to you dated 1/14/14, please document all Active Shooter training you conduct in the national AS file [REDACTED] and the [REDACTED]

b7E



Remember, as the Campus Liaison Agent for your field office, you are responsible for your division's entire AOR. I know that is a lot of territory for one person. My suggestion is to get agents in the RAs assigned to assist you with CLI responsibilities within the RA territories, and you, as the CLA, coordinate the activity throughout the division.

Please let me know if you have any questions.  
Thank you for all your efforts in this arena.

[redacted]  
SSA [redacted]  
Program Manager  
Campus Liaison Initiative

b6  
b7C  
b7E

[redacted]  
Counterterrorism Division - FBIHQ  
[redacted]

**From:** COMBS, CHRISTOPHER H (IR) (FBI)  
**Sent:** Thursday, January 30, 2014 5:44 PM

b7E

**To:** [redacted]  
**Cc:** [redacted] (DO) (FBI); [redacted] (CTD) (FBI); [redacted] (TD)(FBI); [redacted] (FBI); [redacted] (TD) (FBI); [redacted] (DM) (FBI); [redacted] (TD) (FBI)

b6  
b7C

**Subject:** RE: Active Shooter question for the field, others can delete --- UNCLASSIFIED

Classification: UNCLASSIFIED  
=====

Field Active Shooter Team Members:

I am back from my TDY and getting back up to speed on all our Active Shooter (AS) efforts, which is good timing considering there is a new AS push coming from the White House (WH). The Director was given a full program brief by me last week. He was very supportive and would like to see us all continue our efforts and increase them. The Director specifically stated how interested the President is in this effort and the WH staff has repeatedly mentioned to us how astonished they are with our results. We showed the Director some of the positive comments local and state police have sent field offices where training has occurred. The Director was VERY supportive of the FBI conducting training to state and local PDs within field offices. A few points based on the new WH push and the Director meeting:

1. A tasking has come/will be coming from the Training Division (Practical Applications Unit) to your field Tactical Instructors (TI) who became certified ALERRT instructors. This tasking is for them to go out directly to your state and local police and schedule ALERRT training with these departments. We will use FBIHQ AS funds to pay for extra instructors to come and assist if needed. We will also use these travel funds if your instructors incur travel costs. With the number of AS events increasing we must increase the number of schools we hold. Originally we were only doing ALERRT schools with ALERRT instructors but since demand is so high, we will be giving the classes ourselves where needed. Please support these efforts and allow your TIs to conduct these classes and push them to schedule classes. We will be recording these stats and reporting them up the chain all the way. Please make sure you coordinate your efforts with PAU.
  - A. Along this theme we are also starting to conduct regional ALERRT schools in various offices to hit more police. As an example, MW division was able to secure a unused school and hold multiple ALERRT classes at one location. When this was advertised to the area PDs, all the scheduled classes were filled almost immediately. This is a great way to maximize funding, logistics, and hit a larger number of PDs. Again, we will support this effort with funds from HQ. We currently have 7 regional sites in various degrees of progress.



2. We continue to receive requests from departments to attend the 1 1/2 day seminar and the AS TTX. This is especially true from smaller departments not near our headquarters city field offices. Your field offices should schedule more AS conferences and TTXs. As a particular example, to name just one, the Perdue University PD stated how much the conference helped them when they recently had their AS event. Some offices had done multiple conferences around their territory. Some offices did the one required last April and nothing else..... These conferences are making a difference and the more the better. Again, we will support these efforts with FBIHQ funds if necessary. We have held 130 conferences and done 125 TTXs.
3. Based on demand, we created the college AS TTX after the initial push. The response from college police has been great. Please make sure your college liaison agents in the JTTFs are moving forward with this TTX. We are working with the [redacted] closely on this particular initiative. b7E
4. Research Project. We are working with Texas State University (ALERRT), CJIS, CID, DI, and the WH to compile one comprehensive "gold standard" stat sheet on AS events from 2000-2013. Presently there is no national standard set of numbers on AS that the US Gov't endorses. The FBI currently refers to the ALERRT data which is the best single source to date. We are going to combine their data with all available FBI data and create the standard going forward.

We have all worked projects with limited return, questionably worth the effort we put into it, and geared towards threats we did not feel were realistic. You only have to watch the TV for a week and see that these AS events are increasing in number and deadliness. We are getting great return in local and state police good will, our effort has already helped a number of police handle these terrible incidents, and there is no question the threat is real and increasing. Let's keep driving this ball forward! Thank you for your efforts and support.

Christopher Combs  
Section Chief  
SIOC  
[redacted]

b6  
b7C

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



[REDACTED] RMD)(CON)

b6  
b7C

**From:** [REDACTED] (CTD) (FBI)  
**Sent:** Monday, February 03, 2014 7:01 AM  
**To:** [REDACTED]  
**Subject:** FW: Active Shooter question for the field, others can delete --- UNCLASSIFIED

b7E

Classification: UNCLASSIFIED  
=====

CLAs --

As you can see from the email below, your efforts to train campus public safety on Active Shooter events is recognized and appreciated at the highest levels. Of course, no good deed goes unpunished. You are now being requested to coordinate with your Training Coordinator and the Active Shooter Coordinator in your office to conduct more Active Shooter seminars for campus public safety in your AOR.

As requested in an email I sent to you dated 1/14/14, please document all Active Shooter training you conduct in the national AS file [REDACTED] and the CLI file [REDACTED]

b7E

Remember, as the Campus Liaison Agent for your field office, you are responsible for your division's entire AOR. I know that is a lot of territory for one person. My suggestion is to get agents in the RAs assigned to assist you with CLI responsibilities within the RA territories, and you, as the CLA, coordinate the activity throughout the division.

Please let me know if you have any questions.  
Thank you for all your efforts in this arena.

[REDACTED]  
SSA [REDACTED]  
Program Manager  
Campus Liaison Initiative

b6  
b7C  
b7E

[REDACTED]  
[REDACTED] Division - FBIHQ  
[REDACTED]

**From:** COMBS, CHRISTOPHER H (IR) (FBI)  
**Sent:** Thursday, January 30, 2014 5:44 PM  
**To:** [REDACTED]

b7E  
b6  
b7C

**Cc:** [REDACTED] (DO) (FBI); [REDACTED] (CTD) (FBI); [REDACTED] (TD)(FBI); [REDACTED] (TD) (FBI); [REDACTED] (TD) (FBI); [REDACTED] (DM) (FBI); [REDACTED] (TD) (FBI); [REDACTED] (FBI)

**Subject:** RE: Active Shooter question for the field, others can delete --- UNCLASSIFIED

Classification: UNCLASSIFIED  
=====

Field Active Shooter Team Members:

I am back from my TDY and getting back up to speed on all our Active Shooter (AS) efforts, which is good timing considering there is a new AS push coming from the White House (WH). The Director was given a full program brief by me last week. He was very supportive and would like to see us all continue our efforts and increase them. The Director specifically stated how interested the President is in this effort and the WH staff has repeatedly mentioned to us how



astonished they are with our results. We showed the Director some of the positive comments local and state police have sent field offices where training has occurred. The Director was VERY supportive of the FBI conducting training to state and local PDs within field offices. A few points based on the new WH push and the Director meeting:

1. A tasking has come/will be coming from the Training Division (Practical Applications Unit) to your field Tactical Instructors (TI) who became certified ALERRT instructors. This tasking is for them to go out directly to your state and local police and schedule ALERRT training with these departments. We will use FBIHQ AS funds to pay for extra instructors to come and assist if needed. We will also use these travel funds if your instructors incur travel costs. With the number of AS events increasing we must increase the number of schools we hold. Originally we were only doing ALERRT schools with ALERRT instructors but since demand is so high, we will be giving the classes ourselves where needed. Please support these efforts and allow your TIs to conduct these classes and push them to schedule classes. We will be recording these stats and reporting them up the chain all the way. Please make sure you coordinate your efforts with PAU.
  - A. Along this theme we are also starting to conduct regional ALERRT schools in various offices to hit more police. As an example, MW division was able to secure a unused school and hold multiple ALERRT classes at one location. When this was advertised to the area PDs, all the scheduled classes were filled almost immediately. This is a great way to maximize funding, logistics, and hit a larger number of PDs. Again, we will support this effort with funds from HQ. We currently have 7 regional sites in various degrees of progress.
2. We continue to receive requests from departments to attend the 1 1/2 day seminar and the AS TTX. This is especially true from smaller departments not near our headquarters city field offices. Your field offices should schedule more AS conferences and TTXs. As a particular example, to name just one, the Perdue University PD stated how much the conference helped them when they recently had their AS event. Some offices had done multiple conferences around their territory. Some offices did the one required last April and nothing else..... These conferences are making a difference and the more the better. Again, we will support these efforts with FBIHQ funds if necessary. We have held 130 conferences and done 125 TTXs.
3. Based on demand, we created the college AS TTX after the initial push. The response from college police has been great. Please make sure your college liaison agents in the JTTFs are moving forward with this TTX. We are working with the [redacted] closely on this particular initiative.
4. Research Project. We are working with Texas State University (ALERRT), CJIS, CID, DI, and the WH to compile one comprehensive "gold standard" stat sheet on AS events from 2000-2013. Presently there is no national standard set of numbers on AS that the US Gov't endorses. The FBI currently refers to the ALERRT data which is the best single source to date. We are going to combine their data with all available FBI data and create the standard going forward.

b7E

We have all worked projects with limited return, questionably worth the effort we put into it, and geared towards threats we did not feel were realistic. You only have to watch the TV for a week and see that these AS events are increasing in number and deadliness. We are getting great return in local and state police good will, our effort has already helped a number of police handle these terrible incidents, and there is no question the threat is real and increasing. Let's keep driving this ball forward! Thank you for your efforts and support.

Christopher Combs  
Section Chief  
SIOC

[redacted]

b6  
b7C

=====  
Classification: UNCLASSIFIED



=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

From: [REDACTED] CTD) (FBI)  
Sent: Monday, September 29, 2014 4:03 PM  
To: [REDACTED]  
Subject: Behavioral Analysis Coordinators --- UNCLASSIFIED

b6  
b7C

b7E

Classification: UNCLASSIFIED  
=====

CLAs --

I spent last week with all the NCAVC Coordinators from the field. What a great group of agents. If there are any of you out there who do not know what an NCAVC Coordinator is, I have good news and bad news.

Bad: You should have been coordinating your campus outreach efforts with them, so don't admit out loud that you don't know what one is (just like you're coordinating campus-related activity with WMDCs and SPCs also)

Good: NCAVC Coordinators are re-branding themselves. They are now Behavioral Assessment Coordinators. A little more job descriptive, and easier to remember.

More Good News: They are excellent resources for you and your public safety partners.

The title of their conference was Active Shooter 2.0, although the information presented related to a much broader range of people of concern. They had, and I attended, Active Shooter 1.0 a couple years ago and they were sent home with a presentation about behavioral indicators of a potential active shooter. Active Shooter 2.0 focused on the following -- now that you have identified a person of concern, what do you do with them? The new presentation contains additional information on threat assessment, and now includes very important threat management information. All of the information is directly relevant to campuses.

I have encouraged them to reach out to the CLAs in their home offices and form partnerships. I let them know that you can, and should, be assembling your campus public safety contacts in HQ City and in the RAs for training on a regular basis, which will provide a welcome audience for their new half-day presentation. Your campus contacts are going to find this extremely valuable. This presentation is also valuable for Threat Assessment Teams, Administration, Faculty, and others. I'll leave it to you and your BAU Coordinators to determine the best audiences. I have funding to pay for your travel and the travel of your BAU Coordinator (and any other speakers) to wherever your training occurs.

We also discussed a practice that is working well in the New Haven Division. The BAU Coordinator for NH is also an Assistant CLA. As always, they can provide threat assessment assistance to your campuses on people of concern, and targeted threats (such as bomb threats). Having them as Assistant CLAs also provides a force multiplier for the CLI program in your office. It is very difficult for you to get to every campus in your AOR, so an extra body building relationships is helpful. The CLA would still be responsible for the program, but assistants can help you obtain a broader reach. I work with BAU 2 on a regular basis back here at the puzzle palace, and have found our partnership invaluable.

Here is a link to the BAU 2 website:

[REDACTED]  
b7E

And a link to the NCAVC with a list of all coordinators in the field:

[REDACTED]  
b7E

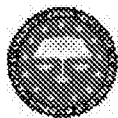


Please let me know if you have any questions.  
Thanks for all the hard work.

[redacted]  
SSA [redacted]  
Program Manager  
Campus Liaison Initiative

[redacted]  
Counterterrorism Division - FBIHQ  
[redacted]

b6  
b7C  
b7E



=====  
Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

From: [REDACTED] (CTD) (FBI)  
Sent: Monday, May 19, 2014 9:59 AM  
To: [REDACTED]  
Subject: FW: Urgent Financial Deadline; New material for Active Shooter Updates --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

From: [REDACTED] (IR) (FBI)  
Sent: Friday, May 16, 2014 3:18 PM  
To: [REDACTED] (IR) (FBI)  
Cc: [REDACTED] (CTD) (FBI); [REDACTED] (MP) (OGA); [REDACTED] (DO) (FBI)  
Subject: Urgent Financial Deadline; New material for Active Shooter Updates --- UNCLASSIFIED

b6  
b7C

Classification: UNCLASSIFIED  
=====

Good afternoon – three items

1. **Funding** - Field offices anticipating the use of AS TR# training **MUST** submit requests to **obligate funds by 06/01/2014**; therefore all offices are requested to finalize all plans for use of FBIHQ Active Shooter funds as soon as possible. This includes travel funds for both FBI personnel and non-FBI personnel. Please ensure your EM is aware of this time deadline, as appropriate.

2. **Presentation/TPs** - Please find attached an updated PPT developed for FBIHQ EM presentations which should not be released outside the FBI but can be used by ADICs, SACs, and ASACs in the field, as they find appropriate. Included in the slide deck is a slide on [REDACTED]

b7E

[REDACTED] These materials will be added to the SIOC Active Shooter web site shortly.



Current\_AS\_with\_t  
wo\_slides\_on\_...



FBI\_Active\_Shoote  
r\_TPs\_updated...

3. **Run/Hide/Fight – School and Health Care Facility application.** DOJ/FBI and Department of Education met with the chiefs of the 50 largest school districts in the US to discuss how to apply RHF in the K-12 environment. The Department of Education, with DHS, DOJ and FBI, are preparing materials specifically to enhance the ability of school administrators, teacher and law enforcement to have valuable discussions on its application. These materials will be forthcoming. In addition, the White House will soon release a guide to aid health care facilities in incorporating active shooter preparedness into facility emergency operations plans. Once released, this too will be provided. Understanding how to best save lives in these unique environment is critical.



Thanks to all of you for the continued work in this arena. The FBI's Active Shooter Initiative continues to gain increased interest from the White House, the media and others. The efforts pushed in the field to pass along lessons learned and best practices are providing a return on your investment, as noted in the talking points.

Regards, [redacted]

[redacted]  
Active Shooter Initiative

[redacted]

b6  
b7C

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



UNCLASSIFIED

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 02-12-2015 BY NSICG/F76M45K62

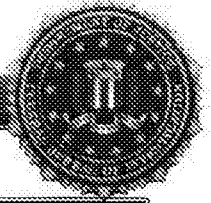
# Active Shooter Initiative



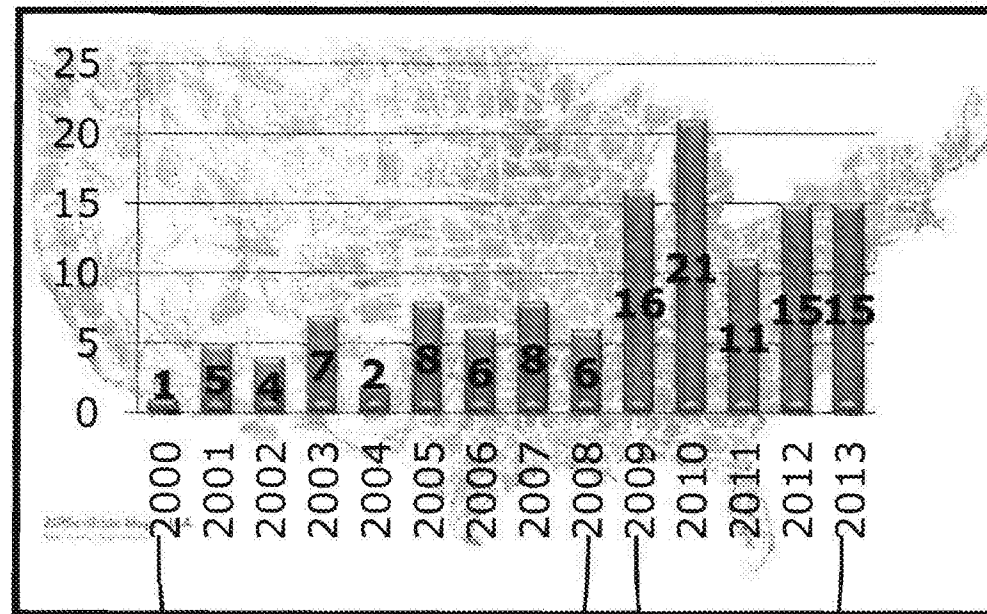
*Federal Bureau of Investigation  
Critical Incident Response Group*

UNCLASSIFIED





## 125 Active Shooter Incidents 2000-2013 (United States) \*



avg 5.22/yr (1 every other month)      avg 15.6/yr (> 1/month)

### 2000-2008

- 324 people shot with 155 killed
- avg. shot 36/yr
- avg. killed 17/yr



### 2009-2013

- 548 people shot with 248 killed
- avg. shot 110/yr
- avg. killed 50/yr



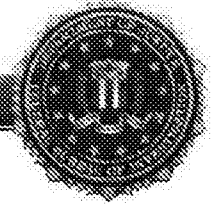
An increase from 36/yr to 110/yr marks a 206% increase in the average number shot per year.

An increase from 17/yr to 50/yr marks nearly a 194% increase in the average number killed per year.

\* No FBI crime statistics are collected for Active Shooter events: Research by J. Pete Blair, Ph.D  
Texas State University (2013)

**Agreed Community Definition for Active Shooter:** Situation where an individual is "actively engaged in killing or attempting to kill people in a confined and populated area"





## Active Shooter Initiatives

- White House “*Now is the Time Initiative*”
  - Interagency working group: DHS/FEMA, DOJ, HHS, ED
  - DOJ tasks FBI to represent all LE on WH working group
- Guidance developed for new Emergency Operations Plans
  - Guides teach the public and organizations how to prepare for emergency situations
  - Guides developed for schools, institutions of higher education, and houses of worship first; health care facility guide to be released in summer 2014
- Established national standard for citizens – *Run, Hide, Fight*





## Active Shooter Initiatives

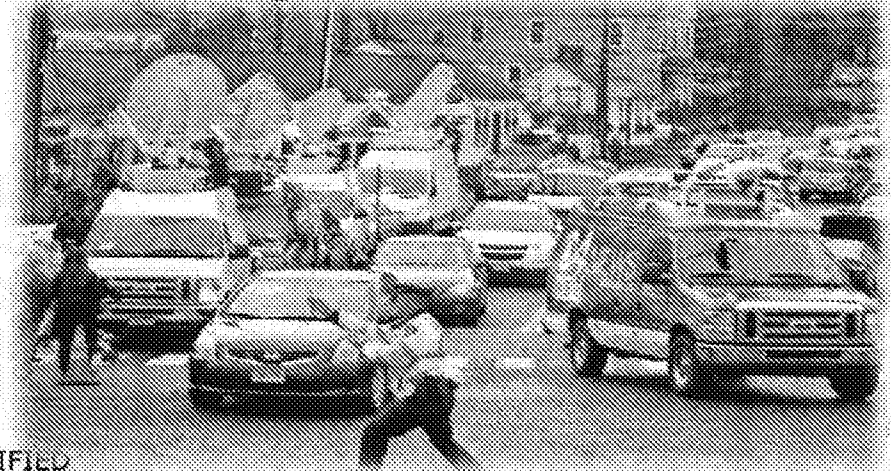
- Promote use of CIRG's Behavioral Threat Assessment Center
  - 200% increase in requests since last year
  - Multi-agency component devoted to supporting the effectiveness of Threat Assessment Teams
  - Dramatic increase in the number of new cases due to public vigilance and the Active Shooter training for LE
  - Approximately 100 new cases in FY11 and FY12. 125 new cases in FY13. On track in FY14 to consult on approximately 200 new behavioral analysis cases
- Passage of Investigative Assistance Act of 2012





## Law Enforcement-Specific Initiatives

- FBI supported Advanced Law Enforcement Rapid Response Training Center (ALERRT), Texas State University. Trained FY 13 to 1<sup>st</sup> Quarter FY 2014:
  - FY 2013 - **1,227** trained in **47** classes from **514** agencies
  - 1<sup>st</sup> Q FY14 - **1,374** trained in **58** classes from **354** agencies
- Conferences for Command Staff
  - To date: **9,648** participants from **4,128** agencies
- TTXs with LE, Fire, EMS
  - To date: **6,387** participants from **2,672** agencies







## Law Enforcement-Specific Initiatives

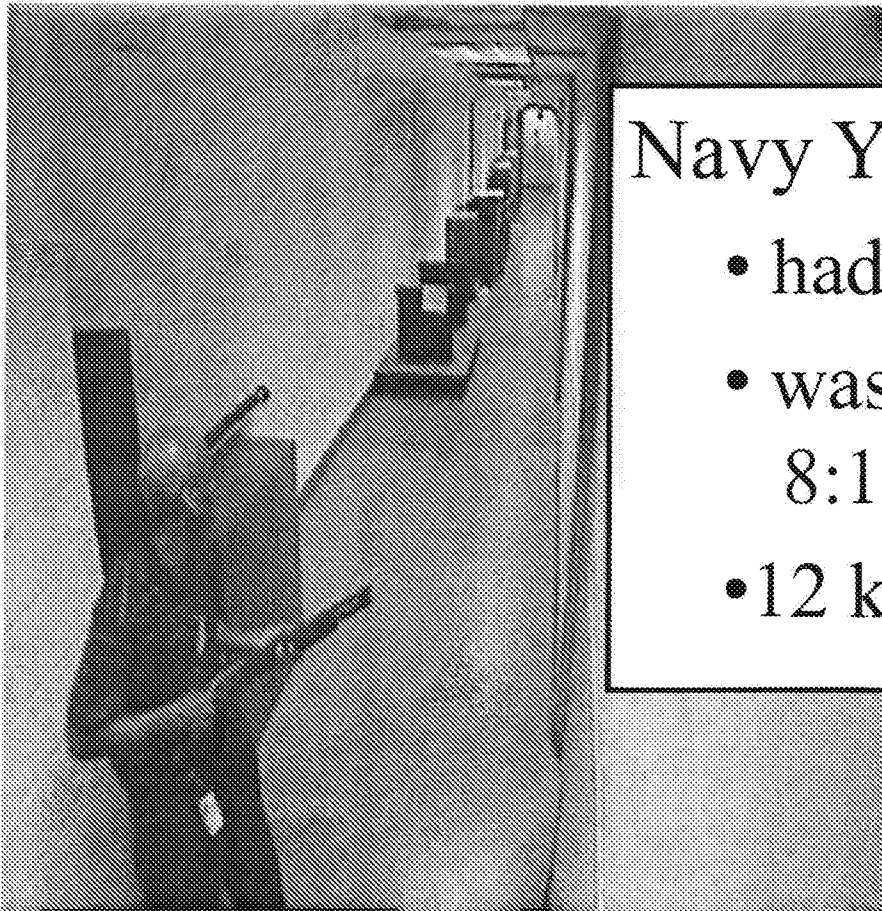
- Aggressive FBI response posture adopted for all FBI field offices
- Increase of Victim Assistance Rapid Deployment Team from  members
- LEO.gov (via LEEP.gov portal) and FBI.gov Active Shooter websites share best practices, lessons learned and subject-specific resources
- Active Shooter Quick Reference Guides for citizens; 500K to date
- Crisis Management Handbooks – more than 25,000 handed out to state and local LE with another 25,000 on order. Smartphone app being developed for distribution. local use.
- HIPPA (Health Insurance Portability and Accountability Act) and FERPA (Family Educational Rights and Privacy Act) pocket guides developed with HHS and ED to assist law enforcement working with health officials and school administrators to timely access needed information

b7E





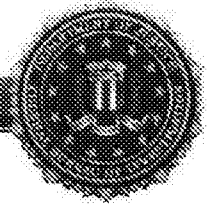
## Increasing Concerns



### Navy Yard Shooter

- had no specific target
- was on the move from 8:16 to 9:25 a.m.
- 12 killed, 3 wounded

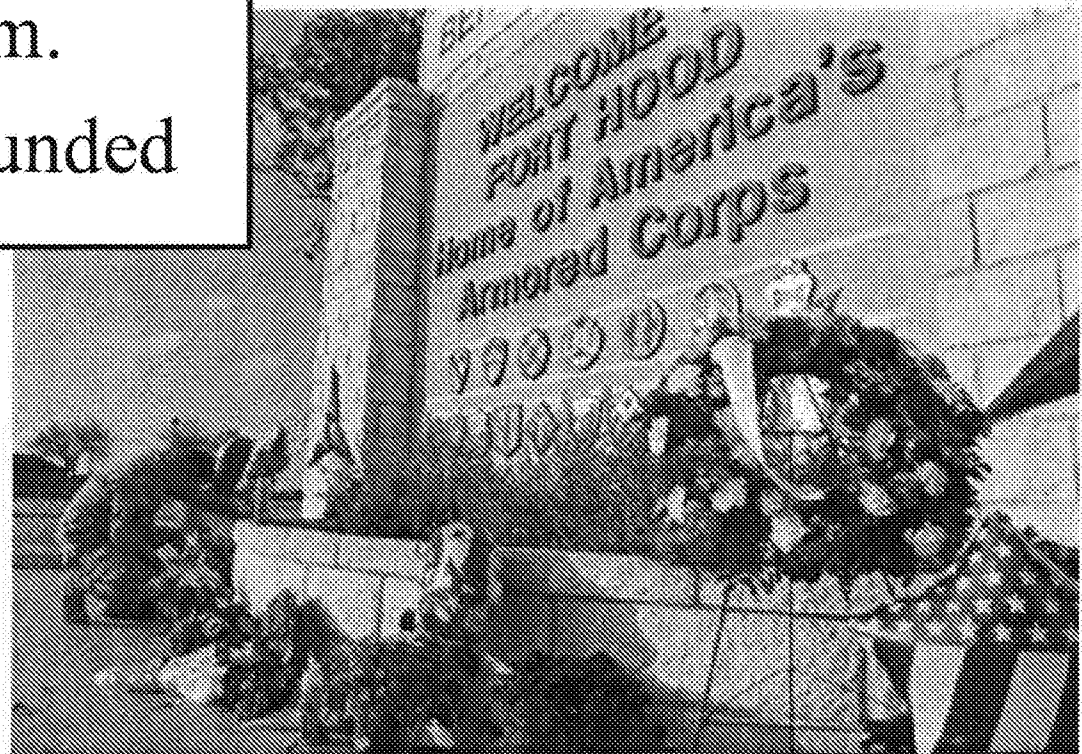




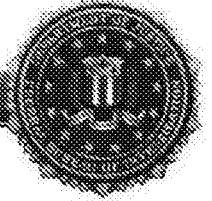
## Increasing Concerns

### Fort Hood Shooter

- was on the move from 4:16 to 6:03 p.m.
- 3 killed, 16 wounded







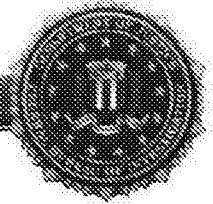
## Increasing Concerns

### Boston Marathon Bombing

- IED
- Multiple actors
- Multiple targets
- Public venue







## Return on Investment

- January 2014 – shooting at Purdue University

*“Kudos to the FBI and the active shooter training from last April. ... I can say with 100% certainty the training prepared me for the storm I would experience some nine months later... My only wish is that more agencies would take advantage of the opportunity to attend the training provided by the FBI.”* – Purdue University Police Captain

- April 2014 - Stabbing at Franklin Regional High School, near Pittsburgh – 21 victims.

FBI Director indicates that police chief told him the training *“...saved the lives of children that day...”* because he recalled the necessity to leave emergency lanes clear for ambulances.



## Additional Briefing notes: Active Shooter, 04/15/2014

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 02-12-2015 BY NSICG/F76M45K62

### UPDATED MATERIALS

#### Successes/Return on Investment

Q. What kind of positive impacts have the FBI's active shooter training programs made?

A. Though it is impossible to quantify what has not happened - those who have not died - anecdotal information received by the FBI supports the conclusion that the FBI's Active Shooter Initiative has altered the end results of these incidents in a positive way when evaluating both potential lives saved and improved law enforcement response.

Refer to FBI Director James Comey's recent discussion about lives saved when 20 people were injured on 04/09/2014 at Franklin Regional High School in Murrysville, PA., after a student reportedly ran through a hallway swinging two large knives at those in his path.

*Director Comey's: "You know we've been doing training all over the country on active shooter, and now we're doing training on complex mall attacks," he told about 20 members of the national media at a press gathering on 05/02/2014. The chief from that town, he said, "wanted to make sure that I knew that the FBI's training had saved lives of children that day in a way that he thought might not be obvious to me. One of the pieces of training we've been pushing out is to tell responders to be sure to keep a path clear for ambulances because of the things we've learned from examining past incidents is that the law enforcement responders race up, park their cars at all kinds of angles, and race toward the building, completely blocking the roads. ... One of the things we've been teaching is race up, but somebody needs to command and keep one road clear; and the chief wanted me to know that kids lived who would otherwise have bled out and died that day because he had received that training and he insisted that a lane be kept clear and the ambulances got right up, grabbed the kids who were bleeding badly, and got them out and saved their lives."*

FBI Divisions have reported back similar anecdotes. Three other recent examples include:

b6  
b7C

- In January, Indianapolis Division reported that Purdue University Police Captain [redacted] credited what he learned at FBI Active Shooter commander conference for his office's effective response after one person was killed at the school's engineering building on campus. "Kudos to the FBI and the active shooter training from last April....I can say with 100% certainty the training prepared me for the storm I would experience some nine months later. ... I know without a doubt that the training came rushing back to me during this time while serving as incident command. The training I received greatly aided me in coordinating the response, investigation, recover and in dealing with the media. My only wish is that more agencies would take advantage of the opportunity to attend the training provided by the FBI."
- In March, San Juan Division reported that four days after Virgin Island Police Department (VIPD) officers attended the FBI's Active Shooter classes; VIPD successfully apprehended six of seven individuals involved in a brazen armed robbery of a jewelry store during peak hours with hundreds of tourist in the street. Through newspaper and radio interviews, the VIPD Commissioner attributed their success, in part, to the recent Active Shooter training.
- In March, Memphis Division reported that the Oak Court Mall in Memphis, Tennessee, was reportedly "shut down in less than a minute" when a dispute between a handful of men turned into a shooting incident. Employees recalled and put into play the training they received last fall from the FBI and Shelby County Sheriff's Office, according to information from the sheriff's office.

Other prevented incidents of violence may be attributed to threat management efforts by local, state, and campus safety stakeholders, with support from CIRG's Behavioral Threat Assessment Center (BTAC). Initiated in 2010, the BTAC offers a dynamic multi-agency (FBI, ATE, U.S. Capitol Police, NCIS) and multi-disciplinary approach to mitigating the risk of active shootings and other acts of targeted violence. When a student, employee, or other individual demonstrates concerning behaviors that create a fear of violence, the BTAC is available to collaborate with local officials and render an assessment as to the potential risk. Working in concert with a CIRG-contracted forensic psychiatrist, BTAC agents and analysts concurrently offer a spectrum of investigative, behavioral, and mental health care/caretaking strategies designed to reduce the risk of violence. These strategies often involve mental health care interventions, leveraging of support systems, separation strategies, and other appropriate care to move the individual off of a potential trajectory towards violence. As campus, workplace, and law enforcement Threat Assessment Teams (TAT) emerge and evolve, the BTAC offers operational, training, and research-based support to TATs in the overall effort to prevent active shootings and other acts of targeted violence.



Privacy regulations and the ongoing nature of these threat management cases limit the amount of specific case information that can be revealed. The consumers of BTAC services (local, state, campus agencies) typically retain primary ownership of these cases and of rights of disclosure for same. Comparing Q1 of FY '13 to Q1 of FY '14, the BTAC experienced a 200% increase in the number of requests for assistance. This increase may be due to both increased public vigilance in the wake of several high profile active shootings and law enforcement awareness resulting from the FBI's Active Shooter training.

#### Successes specifically regarding Tourniquet use

**Tourniquets save 2 lives - Philadelphia's police department issued 5,000 tactical tourniquets to police officers.** Two days after receiving his, a Philadelphia officer who came upon a botched armed robbery used his tourniquet to save the robber's life. Another pair of officers saved the life of a man who had fallen from a roof by using the tourniquets they had received three days prior. The Philly Chief had talked with members of the Boston PD who began carrying tourniquets in April after the Boston Marathon bombing. Philly Police Chief Joe Sullivan was quoted in press as saying "Situations like Boston and the Aurora (Colo.) theater shooting have shown us that there are times when officers are the only ones around. We have to adapt to survive, so that's what we're doing."

#### Resources Used/Challenges Identified

##### Navy Yard Shooting – September 2013

###### Shooter:

- was on the move from 8:16 to 9:25 a.m.
- 12 killed, 3 wounded

###### Navy Yard Challenges:

- Multiple agencies responded
- Self-dispatched officers, entering alone
- Plain clothes officers entered; blue-on-blue threat
- Radio interoperability among agencies, absent FBI and Washington DC police
- Varied training protocols
- Building size (260K sq. ft), 3,000 employees

###### FBI Resources - [redacted]

- General Investigative Personnel - [redacted]
- Command and Control - [redacted]
- Evidence Response [redacted]
- Tactical units (SWAT, HRT, K-9) [redacted]
- Technical assets (bomb, audio/video experts, media, computer experts) [redacted]
- Victim assistance personnel [redacted]

b7E

##### Ft. Hood Shooting – April 2014

- Shooter, no specific target, was on the move from 4:16 to 6:03 p.m., 3 killed, 16 wounded
- Shooter drove through base, stopping and shooting inside buildings and from his car.

###### FBI Resources [redacted]

- [redacted] San Antonio Field office personnel
- [redacted] Deployed from other offices
- Laboratory shooting reconstruction team, cellular analysis survey team, mass fatality victim assistance experts
- Six main search sites

b7E

#### BACKGROUND TPs previously released – Updated information is highlighted in yellow.

##### Active Shooter Interagency Definition:

Situation where an individual is "actively engaged in killing or attempting to kill people in a confined and populated area"

##### Investigative Assistance for Violent Crimes Act of 2012

- Gave authority to act and scope of employment protection to the Attorney General and DHS (USSS and HSI) at the request of an appropriate law enforcement official of a state or political subdivision
- Authority to "assist in the investigation of violent acts and shootings occurring in a place of public use, and in the investigation of mass killings and attempted mass killings"
- Mass killing defined as three or more killings in a single incident.



- Unintended Consequence: "Self Dispatching" has caused Unified Command challenges ,safety concerns and an uncoordinated federal response

#### Background on Active Shooter Incident Response Protocols:

Historical Law Enforcement Response to Incidents involved "contain and wait" protocols

- Once specialized tactical teams became more commonplace in the 1960s and 1970s, patrol law enforcement was trained to CONTAIN AND WAIT for tactical teams who were better equipped and trained. After-action prompted a paradigm shift in the past 15 years.
  - e.g: 1984 – San Ysidro, California – McDonald's Restaurant; 21 fatalities, 19 injured
    - Single shooter with 3 weapons
    - Scene contained in 15 minutes; 257 additional rounds fired by the subject after containment occurred
    - 62 additional minutes before SWAT sniper kills subject
  - 1999 – Columbine, Colorado – Columbine High School, 12 killed, 24 injured.
    - SWAT entered school after 40 minutes and found subjects deceased

#### Advice Given To Citizens

- DHS and the FBI support nationally-endorsed *Run, Hide, Fight* preparedness planning.
- This survival strategy is based on detailed research of active shooter events which studied survival rates of potential victims.
- Individuals must train to overcome denial and to respond immediately, including fulfilling responsibilities for individuals in their charge.
  1. **Run:** The first course of action that should be undertaken is to run out of the building and far away and to a safe location. Consider those in your care and do not hesitate because others do. Call 911 when you are safe. The fewer people in a building, the less who might become victims and the faster law enforcement can clear the building and tend to the wounded.
  2. **Hide:** If running is not a safe option, the second option is to hide in as safe a place as possible. Hide in a location where the walls might be thicker and have fewer windows. Turn off lights and electronic devices and stay secreted until law enforcement tells you it is safe to come out.
  3. **Fight:** If neither running nor hiding is a safe option, as a last resort, an individual or group of individuals may, when confronted by the shooter, try to disrupt or incapacitate the shooter by using aggressive force and items in their environment, such as fire extinguishers, and chairs.

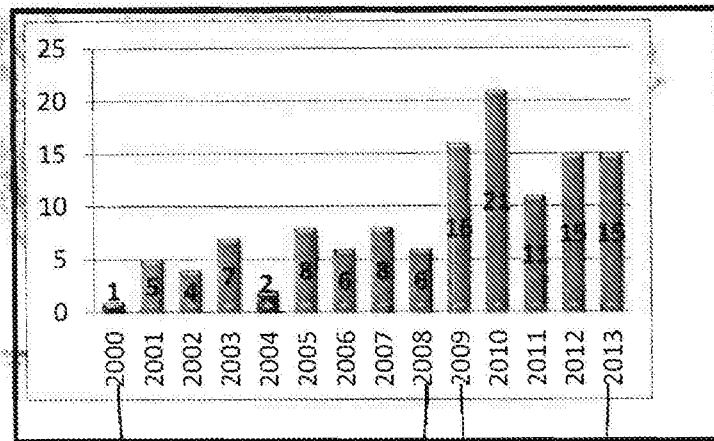
#### ACTIVE SHOOTER STATISTICS

- Nearly every incident is criminal in nature, and involves state and local violations of the law.
- No standardized crime statistics related to active shooter events are currently collected.
- **FBI and Texas State University are currently studying Active Shooter Incidents with updated data availability anticipated to be summer 2014.**
- Research methods and results vary; however, the number of events, people killed and people injured is on the rise.
- J. Pete Blair, Ph.D., Texas State University, 2013: 125 Active Shooter Incidents 2000-2013 (United States) \*

\* 2000-2010, Blair, J.P., Nichols, T., Burns, D., & Curnutt, J.R. (2013). *Active Shooter Events and Response*. CRC Press: New York  
 2011-2013, Blair, J.P. & Martindale, M. H. (2013). *Active Shooter Events in the U.S. Presented at the Annual Community Prosecution Summit of the Association Prosecuting Attorneys in Philadelphia, PA.*



## 125 Active Shooter Incidents 2000-2013 (United States) \*



avg 5.22/yr (1 every other month)      avg 15.6/yr (> 1/month)

**2000-2008**  
 • 324 people shot with 155 killed  
 • avg. shot 36/yr  
 • avg. killed 17/yr

**2009-2013**  
 • 548 people shot with 248 killed  
 • avg. shot 110/yr  
 • avg. killed 50/yr

An increase from 36/yr to 110/yr marks a 206% increase in the average number shot per year.

An increase from 17/yr to 50/yr marks nearly a 194% increase in the average number killed per year.

\* No FBI crime statistics are collected for Active Shooter events. Research by J. Pete Blair, Ph.D. Texas State University (2013)

### WHO IS THE ACTIVE SHOOTER?

- There is no one demographic "profile" of an active shooter
- Individuals engage in both covert and overt behaviors preceding their attacks. They plan, prepare, share, and, in some cases, move on to action.
- Researchers estimate that in 80% to 90% of all instances the shooter displayed detectable behavioral indicators.
- Bystanders represent the greatest opportunity for the detection and recognition of these indicators.
- Successful threat management of a person of concern often involves long-term caretaking and coordination between law enforcement, mental health care, and social services.
- A thorough threat assessment typically necessitates a holistic review.
- While motivations for active shooters are difficult to fully determine, some common "triggers" may include: Loss of significant relationships; Feelings of humiliation/rejection; Changes in financial status; Major adverse changes to life circumstances; Loss of job; Changes in living arrangements.
- Many active shooters were described as "social isolates," who harbored feelings of hate or anger, and/or had some reported contact with mental health professionals. Few had previous arrests for violence.

### PREVENTION

#### Observable Pre-Attack Behaviors

Many offenders who engage in targeted violence may display behaviors during pre-attack planning which may be observable to persons familiar with the offender. While facts differ for each active shooter situation, possible observable warning signs and characteristics might include:

- Development of a real or perceived personal grievance.
- Contextually inappropriate and recent acquisitions of multiple weapons.
- Contextually inappropriate and recent escalation in target practice and weapons training.
- Contextually inappropriate and recent interest in explosives.
- Contextually inappropriate and intense interest or fascination with previous shootings or mass attacks.
- Many active shooters experienced a significant real or perceived personal loss in the weeks and/or months leading up to the attack, such as a death, breakup, divorce or loss of a job.
- Few active shooters had previous arrests for violent crimes.



### Threat Assessment Teams Focused on Prevention

- Best prevention plan - Schools, colleges, houses of worship and private industry should create threat assessment teams or threat assessment units which include mental health professionals, law enforcement and other stakeholders to evaluate information on persons of concern.
- Teams work with law enforcement and often FBI behavioral experts to evaluate the signs of a potentially volatile situation and proactively seek ways to prevent an incident.
- There are currently [REDACTED] b7E
- The FBI leads a multi-agency Behavioral Threat Assessment Center (BTAC) whose members develop dynamic behavioral strategies to disrupt planned active shootings and other attacks. The team includes [REDACTED] b7E
- Each year, the FBI's behavioral experts help develop strategies to assess and disrupt individuals who may be at risk of committing a violent act. Each week the BTAC receives an average of three new cases involving a person of concern, the majority of which involve evidence that the individual is planning or contemplating an active shooting or other catastrophic act of violence.
- Issues traditionally addressed by the BTAC include: active shooters; school, university, and workplace attacks; threats against Members of Congress and public figures; and threatening communications.
- When addressing a person of concern who is on a behavioral trajectory toward an active shooting event, the BTAC works with federal, state, local, and private safety stakeholders to develop and implement a threat management plan to mitigate the violence risk potential.

### INTERAGENCY AND FBI ACTIVE SHOOTER INITIATIVES

In 2013, the FBI joined a White House working group as DOJ's representative on multiple initiatives

- The working group, a collaborative effort with DOJ-FBI, DHS-FEMA, HHS, and ED, resulted in the releases of guides designed to teach the public and organizations how to prepare for emergencies. The FBI authored 11-page active shooter section within guides prepared by the committee which provide direction on how to prepare and react to an incident, and how first responders work to end the threat, save lives, and help victims.
- Guides for schools, institutions of higher education, and houses of worship were also completed. FBI/HHS/DHS currently in final draft of a guide for hospitals and health centers. Guides are available on FBI.gov and other agency web sites.
- Guides established a national Run, Hide, Fight standard protocol for citizens to follow during an Active Shooter Incident

National active shooter response protocol adopted for all law enforcement designed to uniformly train first officers to aggressively pursue a shooter to end the threat and save lives.

- Program created at the Advance Law Enforcement Rapid Response Training Center at Texas State University (ALERTT) and funded by the State of Texas, DOJ, and FBI; 50,000 officers trained since 2002; 1,400 in FY13.
- **Impact of FBI participation in ALERTT training seen in the increase in numbers trained in the first quarter of 2014. 2014 1<sup>st</sup> Q: 58 schools, training 1,374 officers from 354 agencies**
- 125 FBI Tactical instructors attended train-the-trainer classes in FY13 to substantially increase the number of LEO who can be trained in 2014; **FBI Regional offices being set up around the country to pair FBI TIs with locally training officers to increase the number of line officers trained.**

Developed and delivered two-day conferences and table-top exercises in all 56 FBI field office territories to share nationwide best practices and lesson learned in after action evaluations of active shooter incidents.

- Conferences include instruction and discussion with on-scene commanders emphasizing behavioral indicator detection to prevent an attack, as well as current information on IED usage, complex evidence collection techniques, victim assistance resources, and national media management; **9,648 LE participants to date from 4,128 agencies.**
- Table-top exercises bring together representatives from agencies on the scene – law enforcement, fire, EMS, victim services, emergency operations and others – to discuss roles and responsibilities. **6,387 participants; 2,672 agencies.**
- Guidance developed in collaboration with federal agencies, International Association of Chief of Police, Major City Chiefs Police Association, National Sheriffs' Association, International Association of Fire Fighters, and the FBI's private sector Domestic Security Alliance Counsel.
- Distribution of thousands of newly-developed pocket guides and reference documents to LE and private industry.



b6  
b7c

From: [REDACTED] (SE) (FBI)  
Sent: Monday, November 03, 2014 3:29 PM  
To: [REDACTED] (SE) (FBI)  
Subject: FW: RE RMD FOIA --- SECRET//NOFORN

Classification: ~~SECRET//NOFORN~~

~~Classified By: J37J38T63  
Derived From: FBI NSIC, dated 20120629  
Declassify On: 20241231~~

TRANSITORY RECORD  
Last of 3.

b6  
b7C

Classification: ~~SECRET//NOFORN~~

~~Classified By: J37J38T63  
Derived From: FBI NSIC, dated 20120629  
Declassify On: 20241231~~

TRANSITORY RECORD

b6  
b7C

b6  
b7C



Below are some recent and not so recent info on the various FD-542 stats one can claim. Also check out the link which contains additional stat definitions under the document's section.

I've attached a Frequently Asked Questions document which explains how or when some stats might be claimed.

[REDACTED]

b6  
b7C



542\_FAQs\_2009-0  
1-14[2].wpd

From: [REDACTED] (CD) (CON)  
Sent: Thursday, May 21, 2009 8:23 AM  
To: [REDACTED] (SE) (FBI)  
Subject: RE: FD-542 Macro Update

b6  
b7C

~~SECRET//NOFORN~~  
RECORD 319X

Hi [REDACTED]

Thanks and here are some lists, which I have now posted to CD's Intranet [REDACTED] or [REDACTED] though they belong to other divisions. Also, the glossary for the original stats is posted on the [REDACTED] Home Page:

b7E

I probably should have said that in my email :-)



SEMU\_GLOSSARY.wpd SEMU\_LIST.wpd FD 542 Original List.wpd DI\_List\_07-26-2007.wpd DI\_Glossary\_07-26-2007.wpd 542-CI\_STAT\_LIST -REV5-June\_2009... 542-CI-GLOSSARY -REV5-June\_2009...

[REDACTED] PSC/SSA (Ret.)  
Performance Measures & Metrics/FD-542  
Counterintelligence Division  
Executive Staff (CD-5) - FBIHQ Room 4844  
[REDACTED] (desk) [REDACTED] (cell)

b6  
b7C  
b7E

Please take a moment to complete the CD Resource Management Section's Customer Service Satisfaction survey.  
We appreciate you letting us know how we are doing. [REDACTED]

From: [REDACTED] (SE) (FBI)  
Sent: Wednesday, May 20, 2009 3:34 PM  
To: [REDACTED] (CD) (CON)  
Subject: FW: FD-542 Macro Update

b6  
b7C

~~SECRET//NOFORN~~  
RECORD 319X

[REDACTED] Congratulations on your retirement. Both of these lists are very helpful. Do you know who or where I could find a complete list of the FD-542 Stats and Glossary related to [REDACTED] stats. I have some new

b7E



Enjoy your sailing.

b6  
b7C

b6  
b7C

b7E      b6  
b7C

b7E

**Thank you** for your stat collection efforts, ideas for stat updates, challenging but *mostly* solvable questions, and patience with the FD-542 and [REDACTED]. Together, we've made great strides in stat collection since the first major update in October 2005. You have generated hundreds of thousands of data rows that prove your mettle and worth. Best of all, the stats have become an integral and tangible part of your work flow, which is crucial to helping the FBI analyze its investigative activities performance and use that information to manage investigative programs and obtain additional resources that will help you do your jobs even better!

b6  
b7C  
b7E

11

b6  
b7C  
b7E

3



~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations  
DECLASSIFICATION EXEMPTION 1  
SECRET//NOFORN~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations  
DECLASSIFICATION EXEMPTION 1  
SECRET//NOFORN~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations  
DECLASSIFICATION EXEMPTION 1  
SECRET//NOFORN~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations  
DECLASSIFICATION EXEMPTION 1  
SECRET//NOFORN~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations  
DECLASSIFICATION EXEMPTION 1  
SECRET//NOFORN~~

=====  
Classification: ~~SECRET//NOFORN~~

=====  
Classification: ~~SECRET//NOFORN~~



[REDACTED] (RMD)(CON)

**From:** [REDACTED] (SE) (FBI)  
**Sent:** Monday, November 03, 2014 3:28 PM  
**To:** [REDACTED] (SE) (FBI)  
**Subject:** FW: CAMPUS ATTACKS --- UNCLASSIFIED

b6  
b7C

Classification: UNCLASSIFIED

=====  
TRANSITORY RECORD

Per your Email request.

[REDACTED]

b6  
b7C

**From:** [REDACTED] (SE) (FBI)  
**Sent:** Monday, November 03, 2014 12:16 PM  
**To:** [REDACTED] (SE) (FBI)  
**Subject:** FW: CAMPUS ATTACKS ---- UNCLASSIFIED

Classification: UNCLASSIFIED

=====  
TRANSITORY RECORD

Per RMD FIOA Request

[REDACTED]

b6  
b7C

**From:** [REDACTED] (SE) (FBI)  
**Sent:** Thursday, April 22, 2010 5:05 PM  
**To:** SE [REDACTED] SE [REDACTED] SE [REDACTED]  
**Subject:** FW: CAMPUS ATTACKS

Good typology on the subject.

**From:** [REDACTED] (SE) (FBI)  
**Sent:** Friday, April 16, 2010 9:30 AM  
**To:** [REDACTED] (SE) (FBI); [REDACTED] (SE) (FBI); [REDACTED] (SE) (FBI); [REDACTED] (SE) (FBI)  
**Cc:** [REDACTED] (SE) (FBI)  
**Subject:** FW: CAMPUS ATTACKS

b6  
b7C

UNCLASSIFIED  
NON-RECORD

FYI - Attached are BAU reports related to campus attacks that may be of interest to you and local PDs/Campus Security/Police in your AORs.



[redacted]  
From: [redacted] (CTD) (FBI)  
Sent: Friday, April 16, 2010 8:23 AM  
To: [redacted]  
Subject: FW: CAMPUS ATTACKS

b6  
b7C

b7E

**UNCLASSIFIED**  
**NON-RECORD**

CLAs -  
Attached below is the report I sent to you earlier on UNET, along with the talking points and the joint press release. The email below was addressed to your SACs, which included the fact that BAU coordinated this release through our program and all of the CLAs. I didn't want you to be caught unaware. Please let me know if you have any questions.

SSA [redacted]  
[redacted]  
Campus Liaison Initiative  
LX-1-S-400

- desk  
- cell

b6  
b7C  
b7E

From: [redacted] (CIRG) (FBI)  
Sent: Friday, April 16, 2010 10:52 AM  
To: [redacted] (CTD) (FBI)  
Subject: FW: CAMPUS ATTACKS

b6  
b7C

**UNCLASSIFIED**  
**NON-RECORD**

fyi.....

SSA [redacted]  
BEHAVIORAL ANALYSIS UNIT J  
CIRG/NCACV

CELL

b6  
b7C

From: BLECKSMITH, ROBERT A. (IR) (FBI)  
Sent: Friday, April 16, 2010 10:49 AM  
To: FBI SAC's  
Cc: [redacted] (DO) (FBI); [redacted] (OPA) (FBI); [redacted] (OPA) (FBI); [redacted] (IR) (FBI); [redacted] (IR) (FBI); [redacted] (IR) (FBI); [redacted] (IR) (FBI); [redacted] (CIRG) (FBI); [redacted] (CTD) (FBI)  
Subject: CAMPUS ATTACKS

b7E

b6  
b7C

**UNCLASSIFIED**  
**NON-RECORD**

Folks - today the attached report will be released via the FBI's Intranet site [redacted] regarding "Targeted Violence Affecting Institutions of Higher Education." It coincides with the attack on Virginia Tech three years ago. Also attached are some talking points regarding the report and the corresponding joint press release. Although we are not looking for you to initiate any media contacts regarding this report, I wanted to make

b7E



sure you were aware of it and its content in case any inquiries come your way. Media inquiries can be referred to the FBI's Office of Public Affairs at 202-324-3691 and additional guidance for your Media Coordinators is available through OPA. Your NCAVC Coordinators will also receive a copy of the report today for distribution and we have coordinated with CTD's [redacted] Campus Liaison Initiative to distribute the report to all FBI Campus Liaison Officers to ensure the widest distribution of this report. Thanks much, Bob

b7E



Campus Attacks Talking Points GPA03-10\_NTAC.  
041610 Release.... WG 04 14 2010.d... doc

Robert A. Blecksmith  
Assistant Director  
Critical Incident Response Group

[redacted] (secure)

b6  
b7C

UNCLASSIFIED

UNCLASSIFIED

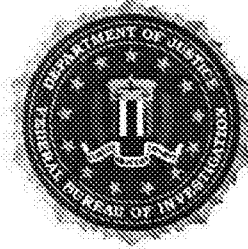
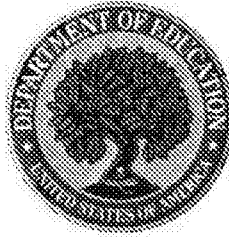
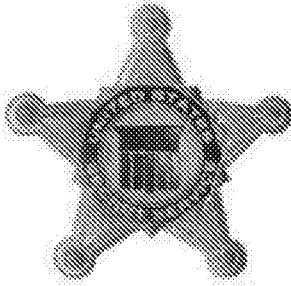
UNCLASSIFIED

UNCLASSIFIED

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED





## Press Release

April 15, 2010  
Contact: 202-406-5708  
GPA 03-10

**NEW STUDY OF TARGETED VIOLENCE AFFECTING U.S. INSTITUTIONS OF  
HIGHER EDUCATION RELEASED**  
*U.S. Secret Service, U.S. Department of Education and Federal Bureau of Investigation  
Collaborate on Joint Effort*

WASHINGTON, D.C. – On Friday, April 16, 2010, the U.S. Secret Service, the U.S. Department of Education and the Federal Bureau of Investigation will release a study of targeted violence incidents on U.S. campuses of higher learning.

The June 2007 *Report to the President on Issues Raised by the Virginia Tech Tragedy* included a recommendation that the Secret Service, Department of Education and the Federal Bureau of Investigation explore the issue of violence at institutions of higher education. This collaborative effort examines the scope of the problem of targeted violence at U.S. institutions.

In total, 272 incidents were identified through a comprehensive search of more than 115,000 results in open-source reporting from 1900 to 2008. The incidents studied include various forms of targeted violence, ranging from domestic violence to mass murder. The findings should be useful for campus safety professionals charged with identifying, assessing and managing violent risk at institutions of higher education.

The study and its findings will be available on each of the agencies' Internet sites: [www.secretservice.gov](http://www.secretservice.gov), [www.ed.gov](http://www.ed.gov) and [www.fbi.gov](http://www.fbi.gov).

###

*EDITOR'S NOTE - For questions concerning the study or its findings, contact the U.S. Secret Service Office of Government and Public Affairs at 202-406-5708, the Department of Education Office of Public Affairs at 202-401-1576 or the FBI Office of Public Affairs at 202-324-3691.*



## TALKING POINTS FOR CAMPUS ATTACKS REPORT

Q. Who prepared the report and why was it prepared?

- This report was prepared by the Secret Service, the Department of Education, and the FBI. This historic collaboration was initiated in the aftermath of the shooting of 32 individuals at Virginia Tech on April 16, 2007. After the tragedy at Virginia Tech, the former Attorney General and Secretaries of ED and HHS recommended to President Bush that the three federal agencies should join forces to study such attacks. They further recommended that the results be shared with those who work to ensure that U.S. colleges and universities remain safe. The three federal agencies forged this partnership, conducted the research, and authored this report to support campus safety professionals and other stakeholders as they work to detect and thwart future attacks on campus.
- The first step in this effort is to understand the key issues and the scope of the problem of "targeted violence\*" at colleges and universities. This report represents the most comprehensive attempt to date to explore the frequency, severity, and nature of campus attacks. We hope that it represents a substantive step in the ongoing effort to keep students, faculty, and staff members safe.

Q. What types of information does the report provide?

- The report provides a significant amount of information on the breadth [number of incidents per decade] and nature of targeted violence [types of violent acts] as well as on key elements of the incidents such as; where incidents occurred, number of incidents per decade and by age group, characteristics and affiliations of subjects, method of attack, and number of injuries and deaths caused.

\* Targeted violence is a term often used by threat assessment and law enforcement professionals to describe an incident of violence where a known or knowable attacker selects a particular target prior to their violent attack. First coined by Robert Fein and Bryan Vossekuil of the USSS in 1995.



many universities function like small cities, and have open borders where people can enter and leave freely. This may suggest that it's very important for campus safety and municipal law enforcement agencies to have open channels of communication and forge effective partnerships.

Q. Will there be any additional reports coming out of the data / information you collected?

- This report, "Campus Attacks: Targeted Violence Affecting Institutions of Higher Education," is the first phase of two phase effort. The second phase will be conducted by the FBI and ED and will involve the thorough and systematic exploration of investigative case files from some of the cases identified in Phase 1. The second phase of this project is intended to provide more in depth information about a select number of cases in order to better identify, assess, and manage persons who pose a risk of violence on campus.

Q. When can we expect the second phase of the report to be released?

- The FBI and ED have recently concluded extensive efforts to gather investigative case files. We will soon commence the analysis of the data, process the results, and then finally write the report and distribute the findings. It is expected that this process will take in excess of a year. We recognize the important and urgent nature of this study and the implications that it has for campus safety. We are working diligently to deliver the best possible product in the least amount of time.



~~SECRET~~

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

[REDACTED] (RMD)(CON)

From: [REDACTED] (SE) (FBI)  
Sent: Monday, November 03, 2014 3:26 PM  
To: [REDACTED] (SE) (FBI)  
Subject: (S) FW: [REDACTED] CLI program --- ~~SECRET~~

b6  
b7C

b1  
b3

Classification: ~~SECRET~~

~~Classified By: J37J38T63  
Derived From: FBI NSIC, dated 20120629  
Declassify On: 20391231~~

=====  
TRANSITORY RECORD

[REDACTED]  
[REDACTED] advised you're the POC on this. Two more coming.

b6  
b7C

From: [REDACTED] (SE) (FBI)  
Sent: Monday, November 03, 2014 12:19 PM  
Cc: [REDACTED] (SE) (FBI)  
(S) Subject: FW: [REDACTED] CLI program --- ~~SECRET~~

b6  
b7C

b1  
b3

Classification: ~~SECRET~~

~~Classified By: J37J38T63  
Derived From: FBI NSIC, dated 20120629  
Declassify On: 20391231~~

=====  
TRANSITORY RECORD

Per RMD FIOA RE Campus Liaison Program

[REDACTED]  
From: [REDACTED] (SE) (FBI)  
Sent: Wednesday, July 11, 2012 12:55 PM  
To: [REDACTED] (SE) (FBI) [REDACTED] (SE) (FBI) [REDACTED] (SE) (FBI)  
(S) Subject: [REDACTED] CLI program

b6  
b7C

b1  
b3

Classification: ~~SECRET~~

~~Classified By: FBI  
Declassify On: 20370711~~

~~SECRET~~



~~SECRET~~

Derived From: ~~FBI NSISC-20090615~~

Gentlemen,

b1  
b3

(U [redacted] lives and works in [redacted] He runs a [redacted] I know he has [redacted]

b6  
b7C

He might be interesting to talk to.

(S [redacted]  
[redacted]

b1  
b3

Also, I thought we could use the Campus Liaison Initiative to talk to various schools around here like Edmonds Community College. It looks like they have a good sized ESL program. The CLI program is a good way to meet staff at ESL schools.

Let me know if you are interested.

[redacted]

b6  
b7C

=====  
Classification: ~~SECRET~~

=====  
Classification: ~~SECRET~~

=====  
Classification: ~~SECRET~~

~~SECRET~~



[REDACTED] (RMD)(CON)

From: [REDACTED] (SE) (FBI)  
Sent: Monday, November 10, 2014 6:44 PM  
To: [REDACTED] (RMD)(CON)  
Subject: [REDACTED] UNCLASSIFIED//~~FOUO~~

b6  
b7C  
b7E

Follow Up Flag: Follow up  
Flag Status: Flagged

SentinelCaseId: TRANSITORY RECORD

Classification: UNCLASSIFIED//~~FOUO~~

ATTORNEY WORK PRODUCT/ATTORNEY-CLIENT PRIVILEGED INFORMATION/DELIBERATIVE  
PROCESS PRIVILEGED DOCUMENT

=====

TRANSITORY RECORD

Good afternoon [REDACTED]

b5  
b6  
b7C

Take Care,

[REDACTED]  
Supervisory Special Agent  
Chief Division Counsel  
Seattle

[REDACTED] main  
[REDACTED] direct

b5

=====  
Classification: UNCLASSIFIED//~~FOUO~~



[REDACTED] (RMD)(CON)

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Tuesday, January 14, 2014 6:56 AM  
**To:** [REDACTED]  
**Cc:** [REDACTED] (IR) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (IR)(OGA)  
**Subject:** FW: Active Shooter question for the field, others can delete --- UNCLASSIFIED  
**Attachments:** Active Shooter conferences.xls

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

CLAs –  
I know you have been conducting Active Shooter TTXs for campuses, and hopefully you have been documenting all of them in the CLI file [REDACTED]. However, I don't know if you have been copying CIRG's Active Shooter file. b7E

Please get with your division Training Coordinator and ensure all TTXs have been accurately recorded and reported to the Active Shooter Program ASAP. This will have a two-fold benefit: 1) it will ensure they have the correct stats for the Director on Friday and 2) it will establish a process to ensure you have correctly documented your efforts and will continue to do so, and therefore won't have to go through this exercise in the future.

Thank you.  
[REDACTED]  
SSA [REDACTED]  
Program Manager  
Campus Liaison Initiative

[REDACTED]  
Counterterrorism Division - FBIHQ  
[REDACTED]

b6  
b7C  
b7E

**From:** [REDACTED] (DM) (FBI)  
**Sent:** Tuesday, January 14, 2014 5:35 AM  
**To:** [REDACTED]  
**Cc:** [REDACTED] (DO) (FBI)  
**Subject:** Active Shooter question for the field, others can delete --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

Good morning from FBIHQ

CIRG executives are scheduled to brief the Director Friday on progress on Active Shooter Initiatives. In preparation, we have gathered the latest statistics on the number of conferences and TTXs from each field office. These have been compiled from activities reported to the active shooter file established for this purpose last year: [REDACTED] b7E

[REDACTED] I have attached the summary of statistics for each field office to review and check for accuracy, as desired. The spreadsheet has a summary sheet on the front and several tabs reflecting the monthly activities of each office, which we hope makes it easier to verify each office's training activities.



Be advised, we are aware and will note that the statistics only include the conferences and TTXs as designed by FBIHQ, and are not reflective of the many other activities recorded in support of the active shooter initiative. These include individual presentations by agents, presentations on behavioral issues, and the many joint presentations in support of local, DHS and other agencies efforts. Those efforts will be noted in talking points.

If you have additional information which needs to be recorded – including scheduled but not yet held conferences and TTXs - please email [redacted] as soon as practicable so that can be included. Also ensure the activity is documented in the listed file when completed. Our goal is to provide the most accurate information available and reflect the excellent and long-standing efforts which have taken place and continue to take place in all of our offices.

b6  
b7C

Training coordinators, please ensure your FO ASAC responsible for this initiative is aware of this email.

As always, if you would like to be removed from this email list, please send me a note and I'll take care of that.

[redacted]  
Active Shooter Initiative  
[redacted]

b6  
b7C

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

From: [REDACTED] (CTD) (FBI) b6  
Sent: Monday, January 06, 2014 1:24 PM b7C  
To: [REDACTED] b7E  
Cc: [REDACTED] (WF) (FBI); [REDACTED] (CD) (FBI); [REDACTED]  
[REDACTED] (SC) (FBI); [REDACTED] (CTD) (FBI); [REDACTED] (CTD) (FBI)  
Subject: Scam Targeting US Universities --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~

=====

Sent for Approval for RECORD//Sentinel Case [REDACTED] b7E

CLAs --

I have heard from a number of you about a scam which has hit many of the universities with which you work that involves the fraudulent purchase of equipment and supplies.

The FBI has open cases on this nation-wide scam. One of the case agents wrote a summary of the scam which is attached below. It should be distributed to your campus public safety contacts. I will forward a copy to you on UNET to ease the distribution process.

At the end of the summary, the victim universities are instructed to provide the information and evidence to you. The information obtained should be directed to the appropriate case Agent/file as follows:

**Orders of electronics/computer equipment:**

SA [REDACTED] Case [REDACTED]

**Orders of Chemicals, Laboratory or Medical equipment:**

SA [REDACTED] Case [REDACTED]

**Orders using the University of California-Davis information:**

SA [REDACTED] Case [REDACTED]

b6  
b7C  
b7E



Supply Scam on  
CLI stationary ...

It is anticipated your efforts will increase the amount of evidence to more effectively prosecute these cases, and eventually reduce the number of victims.

Thank you for your assistance.

[REDACTED]  
SSA [REDACTED]  
Program Manager  
Campus Liaison Initiative

b6  
b7C  
b7E

[REDACTED]  
Counterterrorism Division - FBIHQ  
[REDACTED]



\*\*\*\*\*

Classification: UNCLASSIFIED//~~FOUO~~



[REDACTED] (RMD)(CON)

From: [REDACTED] (CTD) (FBI)  
Sent: Tuesday, November 19, 2013 9:12 AM  
To: [REDACTED]  
Subject: Active Shooter Coordinator Roster --- UNCLASSIFIED

b6  
b7C

b7E

Classification: UNCLASSIFIED

=====  
CLAs –  
If you would like to know who the Active Shooter Coordinator (ASC) is in your field office, you can now find the entire roster on the Active Shooter website:

[REDACTED]  
If you look on the right side bar, under "Resources", there is "Field Office Active Shooter POCs" – this is the list of the POCs in each office.

b7E

You should be working with the ASC in your office to schedule AS seminars, campus TTXs, and ALERRT Training for your campus public safety partners as set out in the EC below:



Campus-Related\_  
Active\_Shooter\_...

Thank you.

[REDACTED]

b6  
b7C

=====  
Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Thursday, November 14, 2013 1:34 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED] (HRD) (FBI) [REDACTED] CD)(FBI)  
**Subject:** FW: College Rx Initiative --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

CLAs -

I wanted to give you a heads up on something that has popped up regarding the College Rx Initiative detailed below.

The College Rx Initiative is simply a powerpoint presentation that was developed by WFO by their Health Care Fraud squad for colleges in WFO territory to address a growing issue on college campuses. I have not yet reviewed the powerpoint, but it sounds like a worthwhile presentation. OPA got wind of it and decided to do a story on it. Since the story was published, WFO has forwarded its powerpoint to approximately 100 people in field offices around the Bureau.

I am getting calls that "FBI Agents" are on campuses giving presentations regarding "drug problems," and the Campus Public Safety Chiefs have not been notified prior to the visit. To ensure we don't have random FBI personnel showing up on campuses providing presentations without coordination with the appropriate officials, I suggest you reach out to people in your office to remind them you and the CLI exist, and you're happy to coordinate contact with campuses within your AOR. At a minimum, you should reach out to your Training Coordinator, Applicant Recruiter, Applicant Coordinator, and Health Care Fraud SSA. Those positions appear to be the ones most often utilizing this program.

Please let me know if I can help you with this issue.

I just don't want all your good work to go sideways due to someone making an innocent mistake on a campus.

Again, this is a worthwhile program, we just need to ensure it is properly coordinated and executed.

Thanks.

[REDACTED]  
SSA [REDACTED]  
Program Manager  
Campus Liaison Initiative

b6  
b7C  
b7E

[REDACTED]  
Counterterrorism Division - FBIHQ  
[REDACTED]

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Thursday, October 24, 2013 8:49 AM  
**To:** [REDACTED]  
**Subject:** College Rx Initiative --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

CLAs -

Another resource:



## College Rx Initiative Targets Students

by [redacted] OPA

Image Caption

Page Content

b6  
b7C

When SSA [redacted] supervised the applicant squad at Washington Field Office (WFO), he couldn't help but notice the number of young professionals turned down for jobs with the FBI due to prescription drug abuse and misuse.

Today, SSA [redacted] supervises Health Care Fraud Squad CR-19, Criminal Investigative Division (CID), at WFO, and he's watched statistics on prescription abuse steadily increase. In December 2011, the University of Michigan's Monitoring the Future study found that, among 12<sup>th</sup> graders, prescription drugs are being abused at a rate second only to the use of marijuana.

"In some cases, it's recreational. But a lot of it is pressure from the students trying to succeed through college," he said.

Under SSA [redacted] direction, an intern with CR-19 this summer—[redacted]

extensively researched these numbers. She found a 2010 study by the National Institute on Drug Abuse that said 7 million Americans reported using prescription drugs for nonmedical purposes. A report by the Institute in 2011 found full-time college students between ages 18 and 22 are twice as likely to use a stimulant for non-medical reasons than those who are in college part time or not at all.

Her research culminated with the creation of a PowerPoint presentation called the College Rx Initiative, designed for college freshmen audiences and their senior class mentors. The Initiative highlights the health and crime dangers associated with prescription medications. It also points out the irony in how abusing the drugs to make good grades could hurt them in obtaining positions with government and private industry employers.

The PowerPoint is available to all field offices. SSA [redacted] hopes other special agents will contact student affairs departments at colleges and universities in their own areas of responsibility to schedule presentations. He said it works best if it is shown during orientation to the freshmen class and to seniors assigned to mentor them.

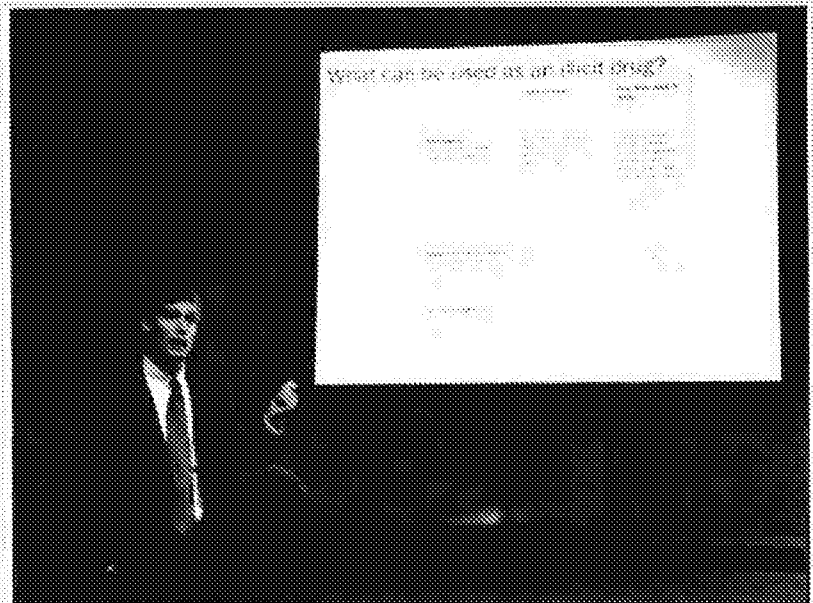
So far, students at Georgetown, American, and Catholic universities have attended College Rx Initiative presentations.

"They were very receptive," said SA [redacted] CR-19, WFO, who gave a presentation at Georgetown University. "I think a lot of them were surprised at the restrictions the government can put on past drug use."

He said information about the effects that prescription drug abuse and misuse can have on their future careers seemed to resonate more with his audience than warnings about health risks and jail sentences. Some, he said, were just surprised to find out it was a crime.

"Kids don't see them the same as street drugs," SA [redacted] said. "It was a little eye-opening to them that handing out Adderall (a drug commonly used to treat ADHD) to friends before an exam could be considered drug dealing."

Studies conducted by the National Institutes of Health back this up. In one interview, a 20-year-old said, "I think prescription drugs sound safer." And a 19-year-old told researchers, "Some people think



SA [redacted] speaking at Georgetown University

b6  
b7C

b6  
b7C



prescription drugs aren't as harmful as street drugs because they are made by somebody who knows what they are doing...They weren't made in somebody's house and they were tested and FDA approved." The College Rx Initiative illustrates how untrue this belief really is. A National Institute on Drug Abuse study reports that in 2007, the number of overdose deaths from prescription opioids outnumbered deaths from heroin and cocaine combined. Misuse and abuse of medications can cause organ damage, heart attack, addiction, and even death.

And unless students become educated about the repercussions, all of these numbers, SSA [redacted] said, are predicted to go up.

If you would like a copy of the College Rx Initiative PowerPoint presentation to use in your area of responsibility, click here. Or, for more information, email SSA [redacted] at [redacted]

b6  
b7c

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



#### OVERALL PROGRAM

- The **FBI Active Shooter program** is designed to train and provide information to departments **from the patrol officer or deputy on the street, to the executives running the command center during an event.**
- Though 98% of these events involve state and local crimes, the FBI provides support to local departments in nearly every instance, **uniquely positioning the FBI to gather best practices and lessons learned.** Why are we at these incidents? It's not a capability problem, it's a capacity problem for the local departments.
- Federal, state and local responders learn more and better ways to do things after every shooting. Through ongoing conferences and tabletop exercises in our 56 field offices, we are **uniquely position to quickly spread best practices and lessons learned to state, local, federal, tribal and campus law enforcement officers.**
- The FBI and the Department of Justice program, which provides logistical, financial and other support to victims, has uniquely position our experts to **gather advice from victims** as well. We are sharing with law enforcement these concerns as well so that first responders better support victims once an incident occurs. Most important, they have told us they want privacy, security and information; often referred to as **Comfort, Kleenex and cold water.**

#### PREVENTION

- **No profile** exists for an active shooter; however, research indicates that as much as **80% to 90% of the times, those intending targeted acts of violence display signs or indicators.**
- These individuals engage in both **covert and overt behaviors preceding their attacks.** They consider, plan, prepare, share, and, in some cases, move on to action.
- The **FBI behavioral experts** are available 365 a year to work with law enforcement around the country to develop **strategies to assess and disrupt individuals** who may be at risk of committing a violent act.
- **Best prevention plan** - Schools, colleges, houses of worship and private industry should create **threat assessment teams or threat assessment units which could include mental health professionals, law enforcement and other stakeholder** to evaluate information on persons of concern. These teams work with law enforcement and often FBI behavioral experts to evaluate the signs of a potentially volatile situation and proactively seek ways to prevent an incident. Each year, the FBI's behavioral experts help develop strategies which turn an individual off of a destructive path.

#### CITIZENS

- We urge them to look to the **FBI's active shooter web site** to see how they can be better prepared, in part by learning the nationally-adopted plan referred to as **RUN, HIDE, FIGHT.** This survival strategy is based on detailed research of active shooter events which studied survival rates of potential victims.
- Individuals must train to overcome denial and to respond immediately, including fulfilling responsibilities for individuals in their charge.
  1. **Run:** The first course of action that should be undertaken is to run out of the building and far away and to a safe location. Consider those in your care and do not hesitate because others do. Call 911 when you are safe. The fewer people in a building, the less who might become victims and the faster law enforcement can clear the building and tend to the wounded.
  2. **Hide** If running is not a safe option, the second option is to hide in as safe a place as possible. Hide in a location where the walls might be thicker and have fewer windows. Turn off lights and electronic devices and stay secreted until law enforcement tells you it is safe to come out.
  3. **Fight:** If neither running nor hiding is a safe option, as a last resort, an individual or group of individuals may, when confronted by the shooter, try to disrupt or incapacitate the shooter by using aggressive force and items in their environment, such as fire extinguishers, and chairs.

#### ALERRT

- It takes **less than a second to shoot two or three rounds** from a handgun and many more rounds will come from an automatic weapon which can carries many more rounds. Because of that, every second saved, may saves lives.
- **Every law enforcement officer in America could be the first officer on the scene when the shooting begins. They all need to be ready.**
- The FBI adopted ALERRT training to ensure consistency nationally in responses. When the shooting starts, officers from every available law enforcement agency respond and a consistent protocol keeps officers and citizens safer. Other programs won't achieve these objectives.
- With the advancement in equipment and specialized training such as bomb experts and SWAT operators, some people might argue that not everyone needs this training or that only tactical experts should engage a shooter. We know now, from research of 100-or-so active shooter incidents during the last 13 years that the best way to save lives is to find and engage the shooter or shooters as soon a possible to end the threat.



- The FBI has 125 tactical instructors trained in the ALERRT protocol and we are working with hundreds of other similarly-trained state, local, tribal and campus law enforcement tactical instructors across the country with a **goal to provide this free training to every officer.**
- Our **biggest impediment** to increasing training is **funding.** FBI so strongly believes this training from patrol officers to chiefs is needed to share lessons learned and best practices

#### **Additional support for questions involving behavioral indicators**

1. No profile exist for an active shooter, however, studies find in 80% to 90% of all instances someone knew something.
2. While motivations for active shooter incidents are difficult to fully determine, some common "triggers" may include: Loss of significant relationships; Feelings of humiliation/rejection; Changes in financial status; Major adverse changes to life circumstances; Loss of job; Changes in living arrangements.
3. Many active shooters were described as "social isolates," harbored feelings of hate or anger, and/or had some reported contact with mental health professionals. Few had previous arrests for violent
4. Many offenders who engage in targeted violence may display certain behaviors during pre-attack planning. These predatory behaviors may be observable to persons familiar with the offender.
5. While facts differ for each active shooter situation, possible observable warning signs and characteristics which might be visible might include:
  - Development of a personal grievance.
  - Contextually inappropriate and recent acquisitions of multiple weapons.
  - Contextually inappropriate and recent escalation in target practice and weapons training.
  - Contextually inappropriate and recent interest in explosives.
  - Contextually inappropriate and intense interest or fascination with previous shootings or mass attacks.
  - Many active shooters experienced a significant real or perceived personal loss in the weeks and/or months leading up to the attack, such as a death, breakup, divorce or loss of a job.
  - Few active shooters had previous arrests for violent crimes.

#### **AS Statistics**

Be aware that statistics vary as research in active shooter specific events is in its infancy.

- **Statistics on 35 Active Shooter events in 2012:** 57% of the attackers were insiders (known); 63% of the attackers broadcasted a perceived injustice; 71% of the victims initially targeted were the focus of the perceived injustice; 74% of the attackers entered through the main entrance. 63% of the attacks were over in under 15 minutes, 37% were over in under five minutes; 51% occurred in the workplace, 17% occurred in schools; 17% occurred in a public place. John Nicoletti, Ph.D. (Nicoletti-Flater Associates) as provided to PERF 4/22/13.
- **84 active shooter events 2000-2010:** 37% in business locations; 34% in schools; 17% in outdoor public venues; 41% used multiple weapons; 4% of the attackers wore body armor; Median number of people killed was 2; \*J. Pete Blair, US Active Shooter Events from 2000 to 2010.

#### **School safety statistics**

Violence on **college campuses** have risen at approximately the same rate as college enrollment has risen based on a study by Drysdale, Modzeleski & Simons, 2010, which reviewed campus incidents reported in the last 100 years. For example, there were eight reported incidents of violence in the 1930s when campus population was approximately 2 million, but there were 92 reported incidents of violence in the last decade, when college enrolment was approximately 20 million.

A new report on **K-12 school crime** in America released in July 2013 determined that violent victimization in schools is on the decline. A school safety report by the DOJ's Bureau of Justice Statistics found that though crime went up slightly in 2011, these types of crimes have steadily decreased since 1992. This most likely, in part, because of the increased awareness in mental health care.



[REDACTED] RMD)(CON)

From: [REDACTED] (SE) (FBI)  
Sent: Monday, November 10, 2014 6:46 PM  
To: [REDACTED] RMD)(CON)  
Subject: [REDACTED] UNCLASSIFIED//~~FOUO~~

b6  
b7C  
b7E

Follow Up Flag: Follow up  
Flag Status: Flagged

SentinelCaseId: TRANSITORY RECORD

Classification: UNCLASSIFIED//~~FOUO~~

ATTORNEY WORK PRODUCT/ATTORNEY-CLIENT PRIVILEGED INFORMATION/DELIBERATIVE  
PROCESS PRIVILEGED DOCUMENT

=====  
TRANSITORY RECORD

Good afternoon [REDACTED]

b5  
b6  
b7C

Take Care,  
[REDACTED]  
[REDACTED]  
Supervisory Special Agent  
Chief Division Counsel  
Seattle  
[REDACTED] main  
[REDACTED] direct

=====  
Classification: UNCLASSIFIED//~~FOUO~~

b5



[REDACTED] RMD)(CON)

b6  
b7C

**From:** [REDACTED] (CTD) (FBI)  
**Sent:** Thursday, September 19, 2013 9:52 AM  
**To:** [REDACTED]  
**Subject:** FW: Active Shooter Initiative update - FY14 budget/Media --- UNCLASSIFIED

b7E

Classification: UNCLASSIFIED  
=====

CLAs –  
Information from the Active Shooter Program

**From:** [REDACTED] (DM) (FBI)  
**Sent:** Wednesday, September 18, 2013 3:34 PM  
**To:** [REDACTED] (DM) (FBI)  
**Cc:** [REDACTED] (IR)(OGA); [REDACTED] (DO) (FBI)  
**Subject:** Active Shooter Initiative update - FY14 budget/Media --- UNCLASSIFIED

b6  
b7C

Classification: UNCLASSIFIED  
=====

Good afternoon -

We've had a busy week here in FBIHQ, in CID, CIRG, SIOC and other supporting divisions, as we work on the Navy Yard shootings and discuss active shooter incidents and response. We also know many offices are following leads to support this WFO response and investigation, which is still very active.

Just a quick note on two related topics, and please pass this up to your EM chain, as appropriate, so they are aware for their own budgeting and liaison purposes.

#### Media

FBIHQ's National Press Office continues to receive requests for media interviews on Active Shooter events and the FBI's involvement in these incidents. We encourage these opportunities to educate the public about the important role the FBI plays in supporting state, local, tribal and campus law enforcement when an incident occurs. Attached please find updated Talking Points for executive use and please ensure all interviews are coordinated with your office public affairs specialist and the HQ Office of Public Affairs, National Press Office.



Active Shooter  
TPs 9.18.2013.d...

#### Budget

Despite FY14 budget struggles, FBIHQ remains committed to support FBI offices as well as state, local, tribal and campus law enforcement agencies to strengthen their readiness to deal with active shooter situations. Based on field requests and objectives for the program, CIRG and TD are working on FY14 budget matters to include some level of support for:

- o Limited travel for FBI personnel supporting Active Shooter conferences in FO AORs.
- o Limited hotel expenses for non-FBI, law enforcement executives so they may travel to attend Active Shooter Executive Conferences.



- o travel for ALERRT training conducted by FBI Tactical Instructors in cooperation with ALERRT-trained local agency personnel.
- o Tactical Individual First Aid Kits (IFAKs) for offices who have trained agents in HRD's Care Under Fire protocols.
- o Training support to add to the cadre of victim specialists who are needed to respond to these incidents.
- o Printed support materials for conferences and field use.

As more information becomes available, we will keep the field apprised.

Please reach out to the Active Shooter team if we can provide support for your liaison and training efforts with local law enforcement.



=====  
Classification: UNCLASSIFIED

b6  
b7C

=====  
Classification: UNCLASSIFIED

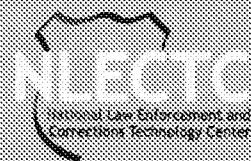




# SHARING IDEAS & RESOURCES



*to Keep Our Nation's  
Schools Safe!*







## INTRODUCTION

Tragic events lead to new prevention and response strategies. We recognize that there are dangers in our communities and in our schools. These realities call for an enhanced focus on safety. The decades-old school fire drill has evolved to active shooter/threat drills as threats have escalated and materialized, often with tragic outcomes.

Our nation is seeking new and innovative ways to keep children and adults safe in school settings. Far from simply developing techniques to respond efficiently to an active incident, public safety officials are also exploring technologies to gauge and prevent potential crises. And they are sharing their ideas and results.

Across the country, entire communities are rallying and dedicating themselves to being proactive in preventing school violence. There is much talk about how existing programs can be reinvigorated, what new technologies can be created and how training tools can be distributed to school resource officers (SROs), administrators and local law enforcement agencies. Modern threats are being addressed with modern technology, strategy and resolve.

The U.S. Department of Justice's National Institute of Justice (NIJ) is a leader in identifying and sharing new training and technology with law enforcement and other first responders. Since Congress passed the Safe Schools Initiative 15 years ago, NIJ has worked collaboratively with other federal agencies on behalf of our nation's law enforcement to answer the call to develop tools and strategies to boost security in our schools. Front-line professionals are working more closely with teachers and administrators, students, parents and community leaders to create alliances that will transform our nation's schools. NIJ, through the National Law Enforcement and Corrections Technology Center (NLECTC), is helping communities gather and share their success stories in this publication and at [SchoolSafetyInfo.org](http://SchoolSafetyInfo.org).

In this guide, you will read about new uses for familiar, standard-bearing technologies such as:

- Advanced Law Enforcement Rapid Response Training (ALERRT)
- NIJ's School Critical Incident Planning Generator (SCIP-G) tool.





- NLECTC System video "It Can Happen Here."
- Free online training from International Association of Chiefs of Police.
- School Safety Audits.

In addition, you will read about new products and apps such as:

- Anne Arundel County (Md.) Police Department's Speak Out app.
- Tucson's Mass Casualty Trauma Kits.
- SmartPhone app for students to communicate with police.
- See-Hear-Report text a tip program.
- Real Time Location Systems (RTLS).

This guide also reports on unique collaborative community efforts that are succeeding in cities and rural areas alike.

It's a new day in the effort to keep schools safe. Law enforcement and public safety officials now team with and count on students, school officials, parents and all concerned citizens to share the responsibility to keep schools safe.

Please use us as a resource and let us know what you are doing to keep your communities safe so we can 'pay it forward' to other communities across our nation.



Keep Safe,

*Michael K. O'Shea*

Michael K. O'Shea  
Senior Law Enforcement Program Manager  
michael.oshea@usdoj.gov

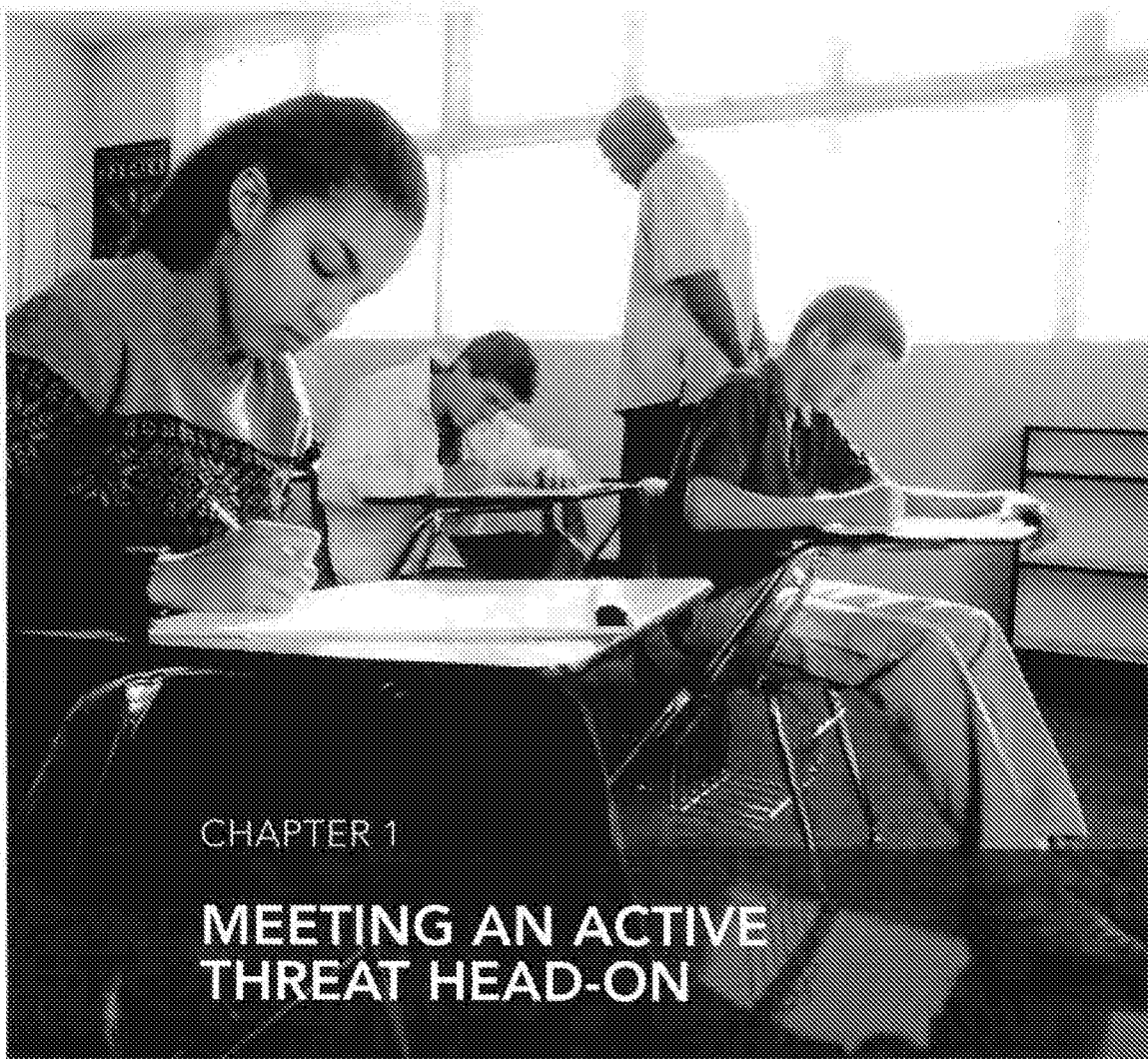




## CONTENTS

Meeting An Active Threat Head-On .....	IV
Students Set the Pace in Learning About School Safety .....	4
Course Teaches Officers How to Administer Aid, Improve Survival .....	8
Finding Ways to Maximize Limited Resources .....	12
After the Shooting Stops .....	16
School Safety Advocacy Council Expands Training Opportunities .....	20
The Immediate First Responder .....	22
Preparing Today for Safety Tomorrow .....	24
Volunteers Come Together to Produce Free Training Video .....	28
It Takes a Village .....	30
Carroll County Involves Officers in School Patrols ...and in Classrooms .....	32
Police School Substations Enhance Safety and Communication .....	36
Police Outfitted With Mass Casualty Trauma Kits .....	38
In-depth Safety Audits Expand School Security .....	42
School Critical Incident Planning – Generator (SCIP-G) Helps Create Coordinated Response .....	46
Smartphone App Provides Alternative Way for Students to Communicate With Police .....	48
Anonymous Reporting and Prevention Platform Helps Stop Trouble Before It Starts .....	50
Tip Line Offers Students a Way to Share Information .....	54
“See-Hear-Report” Reaches Out to Somerset Students .....	58
Real-Time Location System Provides Enhanced Security in Idaho School .....	60
Providing a Direct Connection Between Schools and Law Enforcement .....	64
Real-Time Communications Comes to Oregon School .....	66
Municipal Workers Watch Over Neighborhood Streets .....	70
Video Enhances School Bus Driver Training .....	74





## CHAPTER 1

# MEETING AN ACTIVE THREAT HEAD-ON

By Becky Lewis  
May 2013

### Texas State University-San Marcos

*The next Adam Lanza may not shoot his way through the door of an elementary school. He might get past a school's "buzz for admittance" policy because he's a known visitor; only this time he's carrying a knife and looking for his partner for a deadly reason. Or he might be a student in a small rural school with a gun in his backpack. Or he may find some other way to get past a school's well-thought-out, well-executed safety plan.*



Photo by NTPRO



*However he gets in, if local law enforcement has taken advantage of the free Advanced Law Enforcement Rapid Response Training (ALERRT) Program offered through the Texas State University-San Marcos and funded at a national level by the Bureau of Justice Assistance (BJA), officers will know how to deal with this active threat.*

Since 2002, more than 40,000 law enforcement officers from across the nation have participated in scenario-based training through the university's ALERRT Program, starting with Level I training focused on dealing with active threats. The university's partners, the San Marcos Police Department and the Hays County Sheriff's Office, helped develop the original training program, which has expanded to a national level through the use of state and federal grant funding.

Assistant Director Terry Nichols has been involved in the program since the beginning, when, as a sergeant with the San Marcos Police Department, he worked with Sgt. David Burns, a counterpart at the sheriff's office, to train every officer from the two agencies on dealing with the active shooter threat. Nichols and Burns had received their initial active shooter instructor training from the Texas Tactical Police Officers Association, and after teaching the local officers in Hays County, they appealed to the university for assistance in developing a statewide program. The university then took ALERRT to the national level with the acquisition of BJA funding.

"We've slowly built the program, but Level I remains centered on the active threat," says Nichols. ALERRT offers training sessions at San Marcos, takes them out to other jurisdictions on request and as funding allows, and offers train-the-trainer sessions that spread ALERRT's reach even farther.

"We receive a limited amount of funding from state and federal sources each year to deliver training to law enforcement personnel outside of Texas, and in addition, some states and regions use us to provide training in their areas," Nichols says. To host Level I ALERRT training, the agency must provide a facility such as an unoccupied office or school building with wide hallways and multiple rooms off those hallways. On facility approval, ALERRT allows agencies to enroll between 25 and 30 students, and in return, provides four certified instructors and all the needed materials and equipment.



Photo by Diana Hendricks



## It Can Happen in a Small Town

Galax, Va., an independent city near the North Carolina border, has a population of just slightly more than 7,000 residents. Approximately 400 of them were shopping in a local Wal-Mart late one evening in May 2010 when a call came in about an active shooter in the store. Chief Rick Clark says that his ALERRT-trained officers correctly formed two contact teams, with one moving directly to the threat and the other, to the victim. The shooter, as it turned out, shot himself after shooting his wife, a store employee. He died, and she survived.

"There was no hesitation on the part of my officers. They knew their roles. I've been around a while and I learned the old school way of methodically clearing an area. ALERRT says you go straight to the heart of threat and they did that," Galax Chief Rick Clark says. "We believe in the program. The acronym is ALERRT and I think it gives them more confidence and makes them more alert when they respond."

The leader of the Galax tactical team took ALERRT train-the-trainer training in Lynchburg in 2008, and brought its concepts back to the rest of the agency. Officers can also take ALERRT training at the New River Valley Criminal Justice Academy, which offers in-service training throughout the year and includes ALERRT in its basic recruit training. Galax also hosted a statewide rural-specific training in 2012 that teaches officers how to operate in more wide-open spaces and in wooded areas.

"I believe in training. I believe my folks should have every tool and function necessary to perform their jobs. Even though we're a small agency (24 sworn officers), we face the same issues as they do in Roanoke and Richmond," Clark says.

## It Can Happen Without a Gun

Given the proximity of the Lone Star College System in the Houston area to the ALERRT Training Center in San Marcos, it's no surprise that Lone Star College System Police Department officers have been taking ALERRT training on an ongoing basis for a number of years. Officers at two different campuses put that training to use in 2013, the first a shooting incident on January 22 on the LSC-North Harris campus, the second a multiple stabbing incident on April 9 at the LSC-CyFair campus. (Each campus has an enrollment that approaches 20,000 students, with numerous faculty and support staff present at any given time.)

"The time from when the stabbing call came in until the suspect was in custody was under five minutes. He had run through the hallways of two buildings and assaulted a total of 14 people," says Chief Richard Gregory. "In addition to the ALERRT training our officers received, we had been doing a lot of training for faculty, staff and students on how to respond to an active threat. In fact, some of them had watched a training video earlier that same day, and officers had talked to them about what to do in an active threat situation. In this case, several students actually dragged him to the ground before the officers caught up with





Photo by NYPD

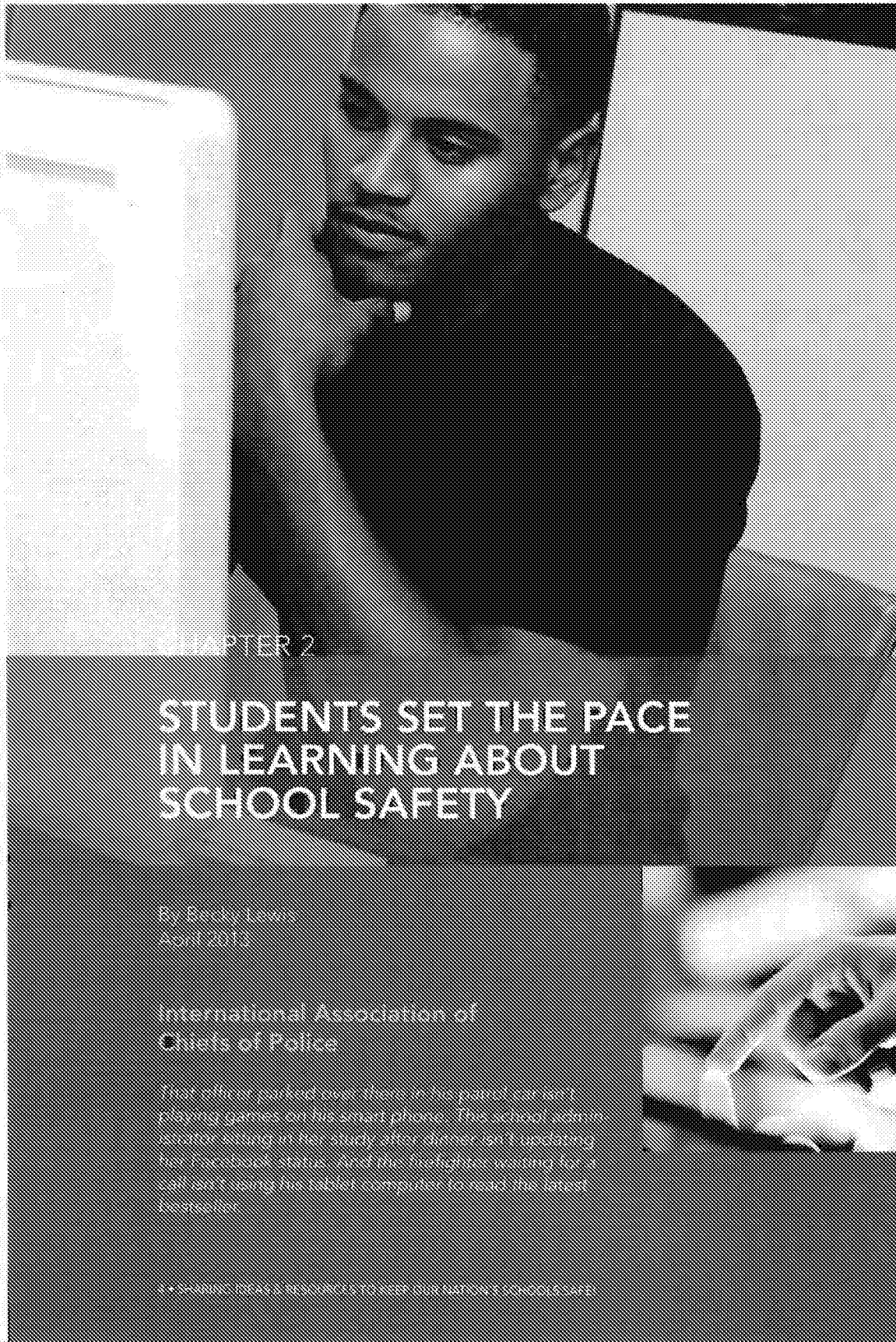
him. When I looked at video of the incident, I saw the officers using the movements that I expected from individuals who had taken ALERRT training."

During the shooting incident, Chief Gregory didn't have to look at video: he was present on the LSC-North Harris campus and witnessed his officers putting their training to use: "The call came out that three people, two students and a facilities employee, were injured. The shooter ran into one of our buildings and the first officer on the scene, adhering to the ALERRT training, went into the building after him before any backup arrived. Two other officers arrived within minutes, and I followed them through the building and observed they were using the ALERRT formation. Officers from two other agencies who also had received ALERRT training arrived and joined right in the formation with no discussion needed. The training allowed officers from three different jurisdictions to search together as a team," Gregory says. (The shooter fled to a wooded area, escaped and was ultimately apprehended a few days later near Dallas, Texas.)

"We initially trained our two firearms instructors to be trainers, because they said it was good active threat training, but also just good officer safety and survival training," Gregory says. "It's just good solid training that we were able to put to good use."

*Read about a Level II ALERRT training class in "After the Shooting Stops" on p.17. For more information on the program as a whole, visit <http://alerrt.org>*





## CHAPTER 2

# STUDENTS SET THE PACE IN LEARNING ABOUT SCHOOL SAFETY

By Becky Lewis  
April 2013

### International Association of Chiefs of Police

*That officer parked over there in his patrol car isn't playing games on his smart phone. This school administrator sitting in her study after dinner isn't updating her Facebook status. And the firefighter waiting for a call isn't using his tablet computer to read the latest bestseller.*

♦♦ SHARPEN IDEAS & RESOURCES TO KEEP OUR NATION'S SCHOOLS SAFE ♦♦



*They're all taking free online School Safety training offered by the International Association of Chiefs of Police, progressing through their selected modules at their own pace.*

IACP and the Office of Juvenile Justice and Delinquency Prevention (OJJDP), a program of the U.S. Department of Justice, Office of Justice Programs, recently launched a series of four introductory-level online school safety trainings. The modules – “Assessing School Safety,” “Forming Your Safe School Planning Team,” “Preparing for a School Crisis” and “Responding to a School Crisis” – provide guidance on creating or enhancing school safety and crisis response plans. The self-paced courses target law enforcement, school officials and allied stakeholders, and students can take one, all four or any other combination, in any order.



Kelly Burke, IACP's Program Manager for Juvenile Justice and Child Protection, says the IACP began developing the program in early 2012 and did not create it as a specific response to the tragedy at Sandy Hook Elementary on Dec. 14, 2012. Based on a two-day classroom training program called Partnerships for Safe Schools, IACP developed the online version in response to the ongoing financial struggle faced by many departments, particularly small and rural ones. Many law enforcement agencies are doing more with less and are not able to release staff to attend classroom trainings – even IACP/OJJDP's no-cost training.

“We wanted to present the training in a way that really engaged the user, so we partnered with a specialist in developing training and online curricula for law enforcement. It's not a static PowerPoint webinar, it uses an interactive self-paced design,” Burke says. “It's designed so it can be used at work, in the car, on smartphones and tablets as well as computers. We've been hearing about e-learning for a while, now we're moving into 'm[obile]-learning.' Instead of having to take eight hours of training in one sitting, this lets them break it down into what's feasible with their schedules. However, they do have to complete all activities before they can advance to the next step and then finally get their certificate.”

One of those activities focuses on dealing with an active threat in a school, but the training also addresses other situations that might require establishment of an incident command post, such as an explosion in the chemistry lab, a student threatening to commit suicide, an abduction on school grounds or a vehicular accident on a nearby street.

“It covers all different types of school crises. Both the classroom and online trainings are based on the Federal Emergency Management Agency crisis model,” Burke notes.





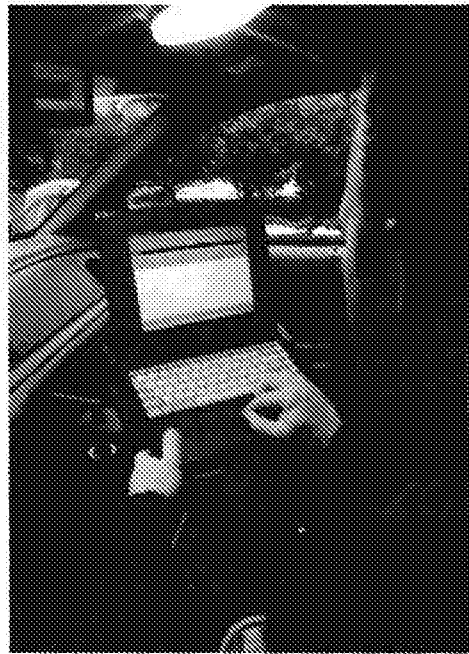
• • SHARING IDEAS & RESOURCES TO KEEP OUR NATION'S SCHOOLS SAFE



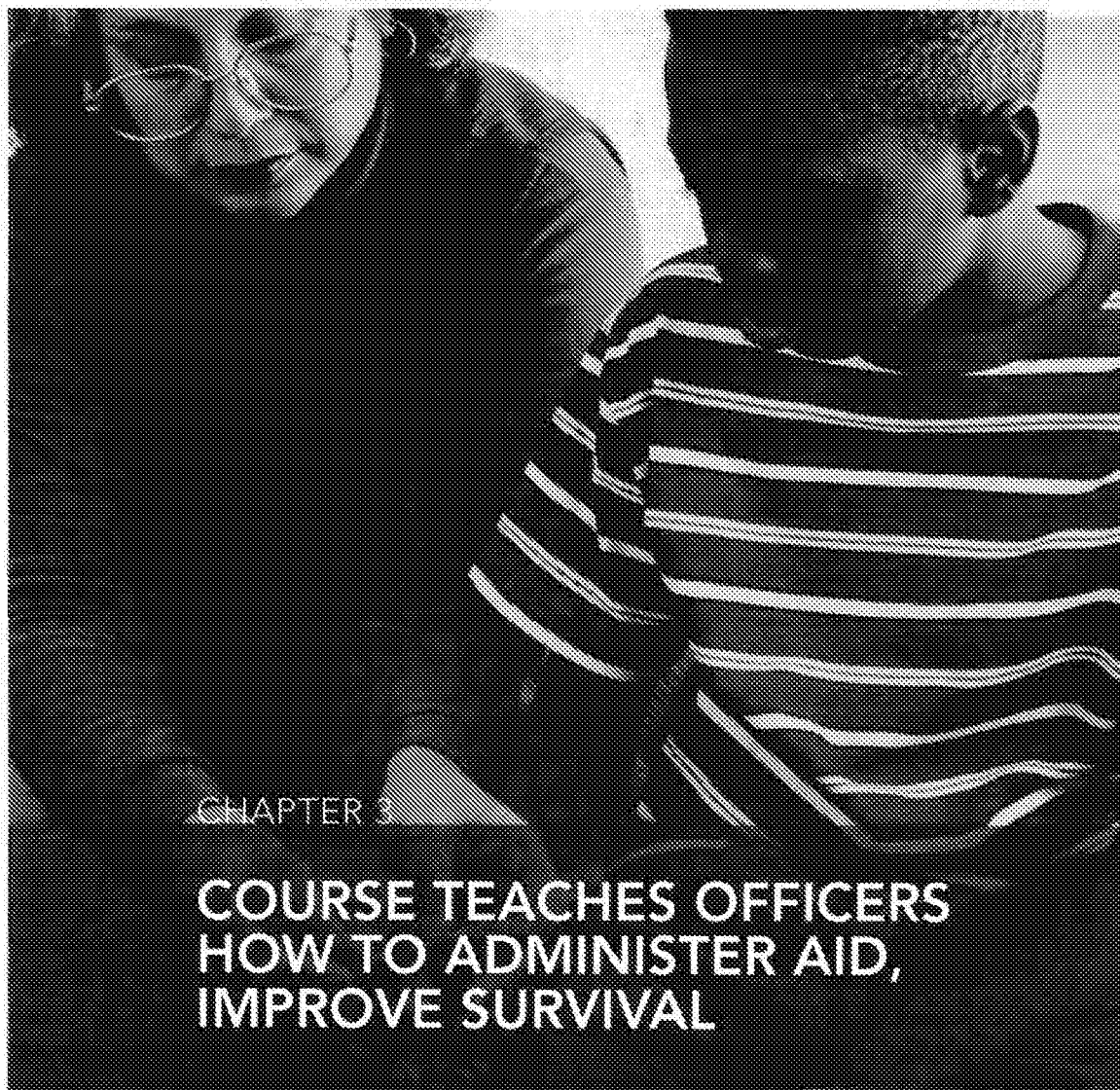
Partnerships for Safe Schools has been delivered 39 times in the past 13 years to more than 1,700 law enforcement and school personnel from 32 states, the District of Columbia and the Bahamas. Based on the initial positive reaction, Burke feels the online component has been, and will continue to be, as worthwhile in terms of bringing school safety to many more practitioners.

The training also targets school administrators, other public safety professionals and community leaders who are involved in school emergency response, with one module specifically focusing on developing a safe school planning team: "We need to recognize who the stakeholders are. It takes more than law enforcement and emergency responders such as fire and EMS. It's administrators, it's teachers, it's mental and behavioral health professionals, it's faith-based leaders in the community, it's neighbors who live near the school and more. They're all stakeholders and the training can benefit all of them."

*For more information and to register, visit:  
<http://elearning-courses.net/iacp>.*







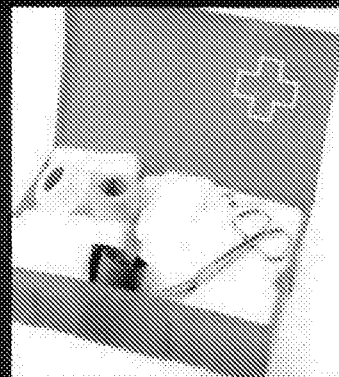
## CHAPTER 3

# COURSE TEACHES OFFICERS HOW TO ADMINISTER AID, IMPROVE SURVIVAL

By Becky Lewis  
August 2013

### National Association of Emergency Medical Technicians

*Evaluation forms filled with column after column of circled "5s" for "Excellent." Those are the marks being earned by the Law Enforcement and First Response (LEFR) Tactical Casualty Care course, a new training program that teaches law enforcement officers and other first responders about basic interventions that could help save someone's life in the precious minutes before emergency medical services practitioners can safely enter a trauma scene.*



8 • SHARING IDEAS & RESOURCES TO KEEP OUR NATION'S SCHOOLS SAFE

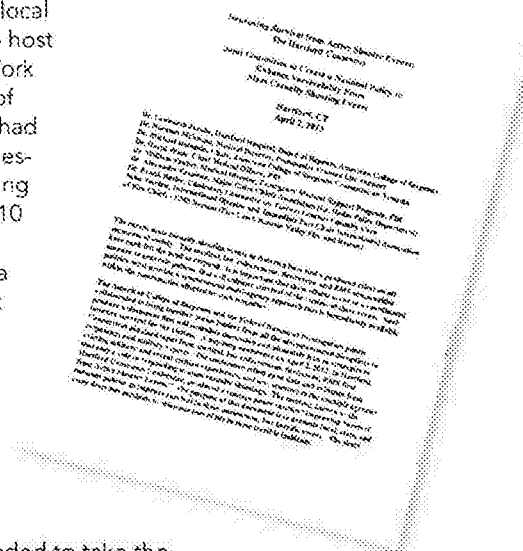


Developed with the Denver Health Department of Emergency Medical Services Education and the Denver Police Department Metro SWAT unit, and offered through the National Association of Emergency Medical Technicians (NAEMT) (<http://www.naemt.org/education/CourseDirectory.aspx>), LEFR uses elements of training provided to U.S. military medics combined with other principles developed by NAEMT's Prehospital Trauma Life Support (PHTLS) Committee. It meets the recommendations of "Improving Survival from Active Shooter Events: The Hartford Consensus Joint Committee to Create a National Policy to Enhance Survivability From Mass Casualty Shooting Events," released by NAEMT on April 2, 2013 (<http://www.naemt.org/Libraries/Trauma%20Resources/Hartford%20Consensus%20Document%20Final%2004-8-13.sflb>)

"We've seen so many incidents nationally – and internationally – in which a large number of casualties have occurred. If you look at many of these incidents, police reach the scene rapidly but EMS entry is delayed until the scene is secure. What we wanted to do is give the police officers who are first on the scene of an active shooter or other mass trauma incident the necessary medical training to perform the very basics of lifesaving care," says Dr. Peter Pons, associate medical director for Pre-Hospital Trauma Life Support at Denver Health Medical Center and an emergency physician. "The military has a two-day advanced level training course and we thought a lot of the principles they teach also made sense for police officers. However, we've adapted it into a one-day civilian course."

Pons already an existing relationship with PHTLS, and worked out an agreement for the Denver agencies to develop the training and field test it on a local level, at which point NAEMT would begin to host and offer the program on a national level. Work started on the project in early 2013, and as of mid-August, the pilot portion of the project had ended successfully and more than 50 LEFR sessions had been scheduled nationwide. Training at the medical center in Denver costs only \$10 per participant to cover certificate printing costs, thanks to a combination of Urban Area Security Initiative and local funding. Costs at other locations around the country will vary; find out more by visiting the NAEMT website listed above, by emailing [education@naemt.org](mailto:education@naemt.org) or by calling (800) 346-2368. For more information on training specific to Colorado, visit <https://www.co.train.org/DesktopShell.aspx>.

Pons says there are no pre-qualifications needed to take the course, which is "really designed for the lay provider. We recognize that police officers frankly have had very little medical training. And the evaluations on the part of the officers who have taken it have been phenomenal."







In addition to those columns filled with the number 5, those phenomenal evaluations have included the following comments:

"Amazing training, especially the way it was taught for non-medical [trainees]. I feel comfortable at this time to be able to get involved with an injury...and at least do what is possible to save someone's life."

"Very informative and helpful scenarios force you to think on your feet."

"Great class. Excellent practicals. Thanks for caring for your brothers in blue!"

"Material was presented in such a fashion that a person with no EMS background such as myself was able to understand."

"Glad to see us being taught to administer aid instead of waiting for rescue."

The aid that participants learn to administer includes the following:

- Immediate steps for hemorrhage control, including external hemorrhage control, direct pressure and wound packing, early use of tourniquets for severe hemorrhage, internal hemorrhage control by rapid evacuation, and transportation to major hospital/trauma center.
- Appropriate application of a tourniquet to an arm or leg.
- Airway control techniques and devices.
- Application of a topical hemostatic dressing (combat gauze).
- Tactically relevant indicators of shock.

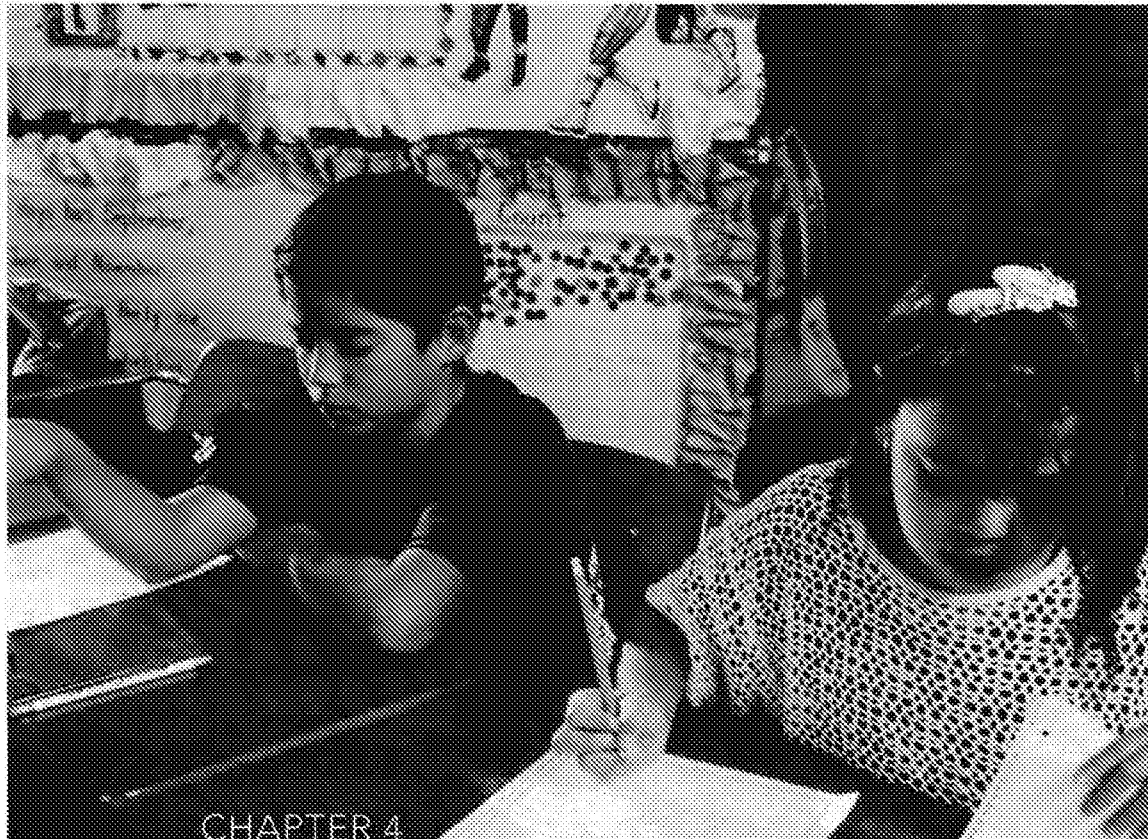
Pons says the morning session consists of a combination of classroom lecture and practice at skill stations, while in the afternoon, participants get a chance to apply the skills they've learned in several scenarios: "Some of them use actors, some use mannequins that bleed. They all replicate scenarios officers could possibly face in the field. We focus on medical care issues, not on tactics. Every police department has its own approach to tactics, and we're not trying to teach them tactics to use in an active shooter or hostage situation. We're teaching them what to do medically if that situation ends with a casualty."





CH. 3. COURSE TEACHES OFFICERS HOW TO ADMINISTER AID, IMPROVE SURVIVAL • 11





## CHAPTER 4

# FINDING WAYS TO MAXIMIZE LIMITED RESOURCES

By Becky Lewis  
May 2013

### Rural Domestic Preparedness Consortium

*In a school safety training session in a metropolitan area, the police chief, the tactical team leader and the bomb squad commander all would likely participate in the class and learn valuable lessons about working together. In a rural area, those three jobs may very well belong to the same person.*





"Crisis Management for School-Based Incidents: Partnering Rural Law Enforcement, First Responders, and Local School Systems," a free training offered by the Rural Domestic Preparedness Consortium (RDPC) and funded by the U.S. Department of Homeland Security, focuses on how to handle school crisis events, including an active shooter situation in a rural K-12 school environment where resources are limited and interagency assistance is many miles away. Instructor Scott Lowry says the most important goal of the training is to teach participants – including school personnel, law enforcement and other first responders such as EMS and fire – to recognize the limits they have as a community and to find ways to mitigate the lack of resources: "People have to take on multiple responsibilities in a moment of crisis and it's important for the community to identify the gaps ahead of time."

One community that recently hosted such a training is the small western Montana town of Libby (population approximately 2,700), located in the Kootenai National Forest between the Cabinet Mountains to the south and the Purcell Mountains to the north. Lisa Oedewaldt, who wears three hats herself (deputy director of emergency management, public health emergency preparedness coordinator and flood plain manager), heard about the training through a local school administrator and first participated in a session in the reservation community of Browning. Oedewaldt was so impressed she then worked with the Montana Department of Disaster and Emergency Services and RDPC to bring a session to Libby on April 1, 2013.



"Scott took our high school (560 students, grades 7-12) and developed a scenario focusing on dealing with an active shooter there. I told him what our area was like, who coordinated with whom and how the agencies worked together. Scott incorporated all of it into our scenario, including how remote we are and how if we had to close the one major highway, we'd be completely cut off," Oedewaldt says. "He made the principal decide to change the way the school does lockdown drills and the local police decide to go from waiting for backup to the first person on the scene goes in. They really changed the way they plan to handle things because of the training."

She adds, "We went through pictures of each school and looked at things like placement of bushes, and he encouraged them to think about ways to improve safety. It was just so interactive and everybody got involved."

"Everybody" included officers from the six-person Libby Police Department, the Lincoln County Sheriff's office, the Montana Highway Patrol and the U.S. Forest





Service police. The latter three agencies have a total of 32 officers for the entire county, which includes two other school districts that have not yet participated in the training.

"In dealing with extreme rural areas like Libby, a lot of the conversation during the day focuses on what they need to do and how to do it with limited resources. In metropolitan areas, where they can pull from the adjoining jurisdictions, the demand on the community is not as great," Lowry says.

In the eight hours of instruction time, Lowry works with rural areas on developing emergency plans that they maintain as living documents, performing a school vulnerability assessment, looking at available assets and developing a strategy for threat assessment management.

"Our philosophy is if we prepare for the worst case scenario, everyone will still respond appropriately to any lesser incidents. We talk about making appropriate decisions, such as when to stay in the classroom and when to go out the window," Lowry says. "We want to educate our teachers to make rational decisions during irrational times so they can further ensure the safety of the children in the classroom."



For law enforcement participants, the objective is to teach them to train in the way they expect to respond, because in an emergency, they will instinctively respond the way they were trained. One of the main objectives of this training is to get law enforcement and school personnel on the same page to ensure collaborative strategies are in place for effective crisis prevention, response and recovery in the K-12 environment.

The training also emphasizes the recovery phase, because, Lowry says, many jurisdictions do a good job with emergency operation plans and lockdown drills, but "what escapes a lot of people is post-incident recovery. When children have experienced a traumatic event, the mental health aspect needs to be engaged immediately thereafter. The ultimate goal is to get back to normalcy as a community, and the mental health portion is critical to that. Chardon High School in Ohio immediately implemented a mental health and recovery phase that should become a model of how to recover from a school shooting."

### About the Course

RDPC offered AWR 148 "Crisis Management for School-Based Incidents: Partnering Rural Law Enforcement, First Responders, and Local School Systems" 316 times and trained 8,925 individuals from May 2009 through May 2013. Requesting agencies must be vetted and, if approved, need only provide a classroom equipped with audio/visual equipment large enough to accommodate between 20 and 40 participants. Interested persons who cannot attend a training session may take a web-based version. More than 900 individuals have taken advantage of the web-based option as of May 2013.

To request this or any other RDPC course, visit <http://www.ruraltraining.org>, select the link for "Request a Course" and complete the online form. You will be contacted to complete the verification process, and receive a date and an instructor. Requests can also be made by calling toll free to (877) 855-RDPC.







## CHAPTER 5

# AFTER THE SHOOTING STOPS

By Becky Lewis  
May 2013

### University of Texas-San Marcos

*The gunshots that filled the halls a few minutes earlier have ended, but the all-clear to bring in the EMS personnel won't come until after the shooter has been taken from the scene and after a final check to make sure he acted alone. While minutes tick away – sometimes just a few, sometimes a couple of hours – blood continues to flow. Blood from wounds that could be life-threatening if not treated right now, by someone already on the scene. Treated by a law enforcement officer who has completed Level II ALERRT training.*





"Terrorism Response Tactics," the second level of the Advanced Law Enforcement Rapid Response Training Program offered by the ALERRT Training Center at Texas State University - San Marcos, takes officers to the next step to take after an active threat has been neutralized. "About two years ago, we realized that officers are getting really good at learning how to deal with an active threat and stop the killing, but they didn't know how to stop the dying after they put the bad guy down. We want to give them the tools to save as many lives as we can," says ALERRT Assistant Director Terry Nichols.

The techniques taught in the course derive from tactical combat casualty care methods developed by the U.S. Army over the past 10 years, and the Army's Dr. Robert Mabry serves as medical adviser to the training: "The chief preventable reason why people die in combat is external hemorrhage from injuries to limbs. We've trained soldiers to deal with life-threatening loss of blood, and ALERRT is now teaching police officers how to pack wounds with hemostatic gauze, how to apply tourniquets, how to position people so they can breathe and not drown in their own blood. ALERRT teaches these techniques at an appropriate level for law enforcement use. We don't need to make law enforcement officers into trauma surgeons, but we can give them effective tools so they can do what a trauma surgeon would do in the same circumstances. If you kill the bad guy, but three kids bleed to death before EMS gets there, the mission has still failed."



Photo by Diana Hendricks

Nichols says the training – which can take place in either a scheduled class at San Marcos or "on the road" at the request of a local jurisdiction – works best if firefighters and EMS personnel from the same jurisdiction all participate. The first day of the class provides instruction for students on basic medical skills including the use of tourniquets, improvising tourniquets, wound packing, bandaging and lifts/draggs/carries. On the second day, students learn triage and link-up procedures, and review tactical considerations for responding to an active shooter. The class includes multiple force-on-force scenarios where officers must first stop an ongoing threat and then experience several ways of dealing with numerous injured victims, including taking the wounded out to fire and EMS as well as providing security for fire and EMS to enter a crisis site.

"The primary concept we want to enforce is what we can do immediately on the scene to save lives, which is mainly hemorrhage control. Officers also have to learn there are some injuries they can't work on, such as a penetrating gunshot wound to the abdomen. That requires an operating room and a trauma team.





They learn how to prioritize which injuries need immediate attention and which ones can wait," Nichols says. "Active threat training is great, but this class is what happens after the shooting stops. It focuses on saving lives and integrating those efforts with fire and EMS."

Nichols says that integration requires philosophical and policy changes, because traditionally, fire and EMS won't enter a scene until it has been secured: "They will have to learn to let law enforcement define what is secure, to trust law enforcement to provide cover and keep them safe. It starts with having a discussion about working together and talking together. If they've trained together, it's going to help build that needed trust."

### Applying Training in Real Life

Law enforcement officers in the state of Texas who complete "Terrorism Response Tactics-Active Shooter Level II" receive a medical kit to carry in their patrol cars that includes a tourniquet, shears, hemostatic gauze, field dressings and sterile gloves. (Students from outside the state receive instructions on how to set up their own kits). One student who has already put his kit to good use is Officer John Mahoney of the New Braunfels Police Department, who found himself called to the scene of major vehicle accident in summer 2012.

Mahoney said he arrived on the scene ahead of the paramedics and found a woman who had her right leg caught between her motorcycle and the pickup truck that struck her. The victim lay on the ground bleeding from a severed major artery, and a bystander exclaimed "she's bleeding out."

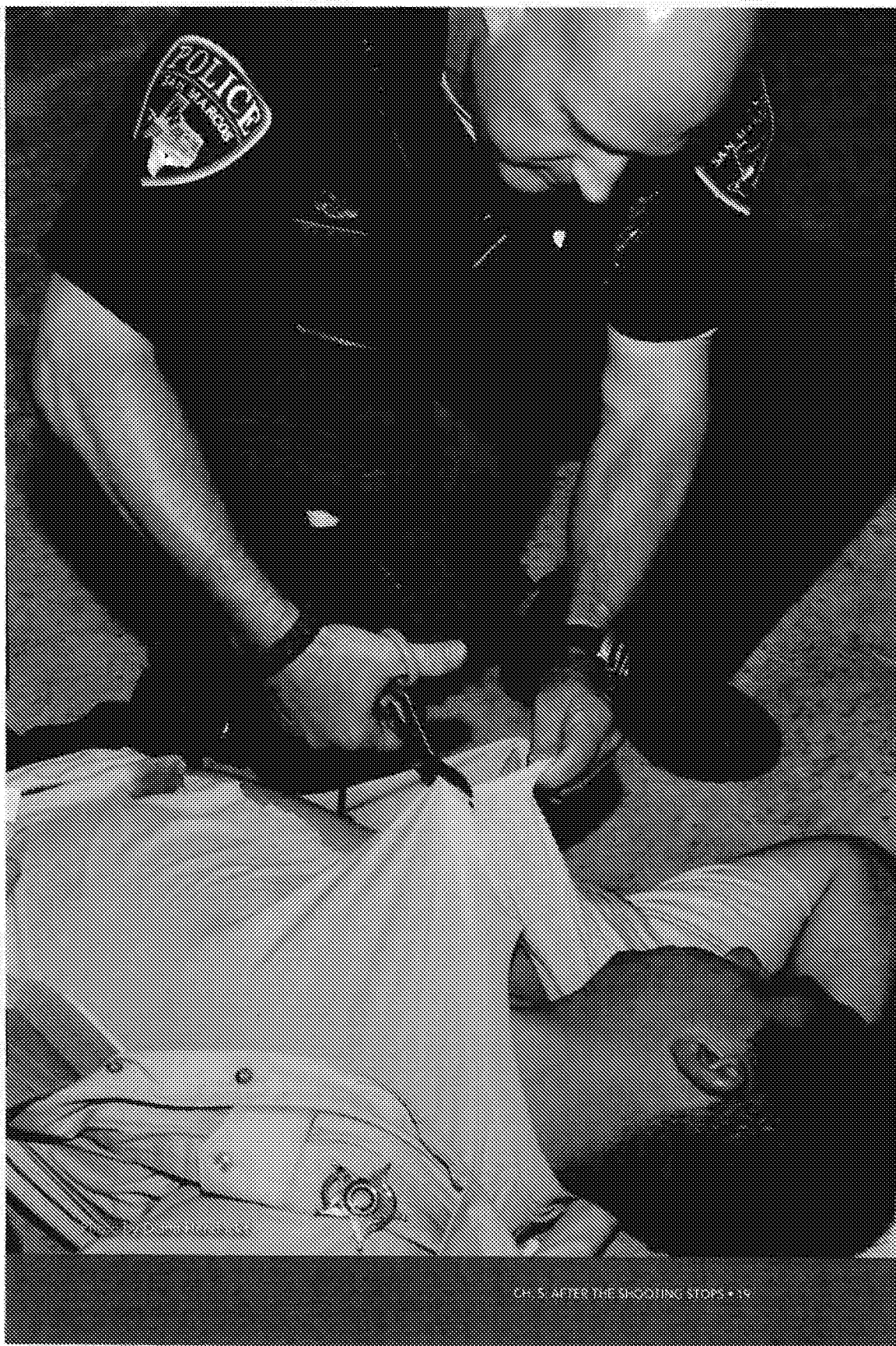
Mahoney retrieved his medical kit and applied a tourniquet to what paramedics later termed a life-threatening injury. He received a departmental award for his efforts.

"My department has encouraged everybody to take Level I Active Shooter training. After going, I learned about other classes and started taking them on my own," Mahoney says.

"Normally at that type of accident we would just provide traffic control, but it had been only a couple of months since I took the training, and after thinking about it for just a moment, I realized that I had the training, I had the equipment and I could help her," he adds.

To read about active threat training, see "Meeting an Active Threat Head-On" on p. IV. To learn more about all of the ALERRT training programs at Texas University-San Marcos, visit <http://alerrt.org/>.









## CHAPTER 6

# SCHOOL SAFETY ADVOCACY COUNCIL EXPANDS TRAINING OPPORTUNITIES

By Becky Lewis  
February 2013

### School Safety Advocacy Council

*The officer parks her squad car in front of the local high school and enters the front door. The students walking the halls between classes aren't alarmed to see her. She drops by often to do some administrative work at her desk in the school office, and students expect to see her mingling with them almost every day.*





In addition to its ongoing training programs, the School Safety Advocacy Council (SSAC) has introduced Law Enforcement Educational Presence (LEEP), a two-day School Safety Certification Course for Patrol and Reserve Officers.

"As a result of the recent tragedy at Sandy Hook, we worked with law enforcement and school administrators from around the country who are subject-matter experts to create this program," says SSAC President Sean Burke. "If law enforcement agencies nationwide stationed an officer in every school, it would take one-third of the sworn officers in the country.

"The basic idea behind LEEP is to get local law enforcement more involved with the schools in their jurisdiction. LEEP promotes the idea that schools can have a satellite office in their buildings where officers on patrol, officers from specialized units, can set up a schedule to work out of that office part time. That way, they get to know the administrators, they get to know the students, they get to know the layout of the building. If an emergency response is needed, there is an officer who knows the school and has a relationship with the students and staff. The majority of the potential school shootings in this country that have been averted were stopped because students provided information to an officer with whom they had developed a relationship."

To learn more about the available training on how to establish a LEEP program in your area, visit <http://www.schoolsafety911.org/index.html>, the SSAC website. The site also offers information on other specialized services and trainings offered by SSAC, which has trained more than 100,000 law enforcement officers and education professionals in the United States and abroad. SSAC also offers the following on a regular basis:

- Basic School Resource Officer Certification Course.
- Advanced School Resource Officer Certification Course.
- Emergency Management Response in the Educational Setting.
- Gangs 101: What Every Educator and SRO Should Know.
- School Law & Liability.
- School Safety Leadership & Supervision.
- When Terror Goes to School -- Understanding the Threat of Terrorism in Today's Schools.

In addition to several specialized trainings on bullying, SSAC holds two national conferences each year, one of them the largest conference on bullying in the United States. The agenda for the other 2013 event focuses on emergency response and school shootings. Details on upcoming conferences can also be found on the SSAC website.

"The unique thing about SSAC is that all of the instructors we employ are subject-matter experts who remain active in the field. That's what sets us apart," Burke says. "There are training programs out there that just focus on school staff, and trainings that just focus on law enforcement, but we bring together the community, the schools and local law enforcement to address school safety and bullying. We see school safety as a community-wide responsibility."





## CHAPTER 7

# THE IMMEDIATE FIRST RESPONDER

By Becky Lewis  
February 2013

### National Association of School Resource Officers

*School resource officers (SROs) are more than just police officers assigned full time to a school. They are the immediate first responders to any incident that happen on campus.*





"The SRO is always the immediate first responder to any and all incidents that happen on campus," says Kevin Quinn, president of the National Association of School Resource Officers (NASRO). "That's a very critical aspect of the job. There's no response time, because we're already here. In the time it would take somebody in the office to pick up a phone, call 911 and tell a dispatcher, who would then relay that information to an officer who isn't familiar with the campus, I would have already walked down the hall and been on the scene."

SROs play two other key roles in addition to covering their beats at the school. They visit classrooms and make presentations on school safety, traffic laws, general law and crime prevention; and they confer with students, parents and family members on legal problems and crime prevention.

NASRO, founded in 1989, provides training and other resources to help SROs perform all of those roles better. The organization offers basic and advanced training for SROs and managers, as well as specialized training in legal issues affecting school safety. Quinn says that requests for training have "exploded" in the wake of the Dec. 14, 2012, shootings in Newtown, Conn., with NASRO scheduling approximately 50 training classes in the first eight months of 2013. For more information on NASRO, its trainings and its annual conference, visit the NASRO website at <http://www.nasro.org> or call (888) 316-2776.

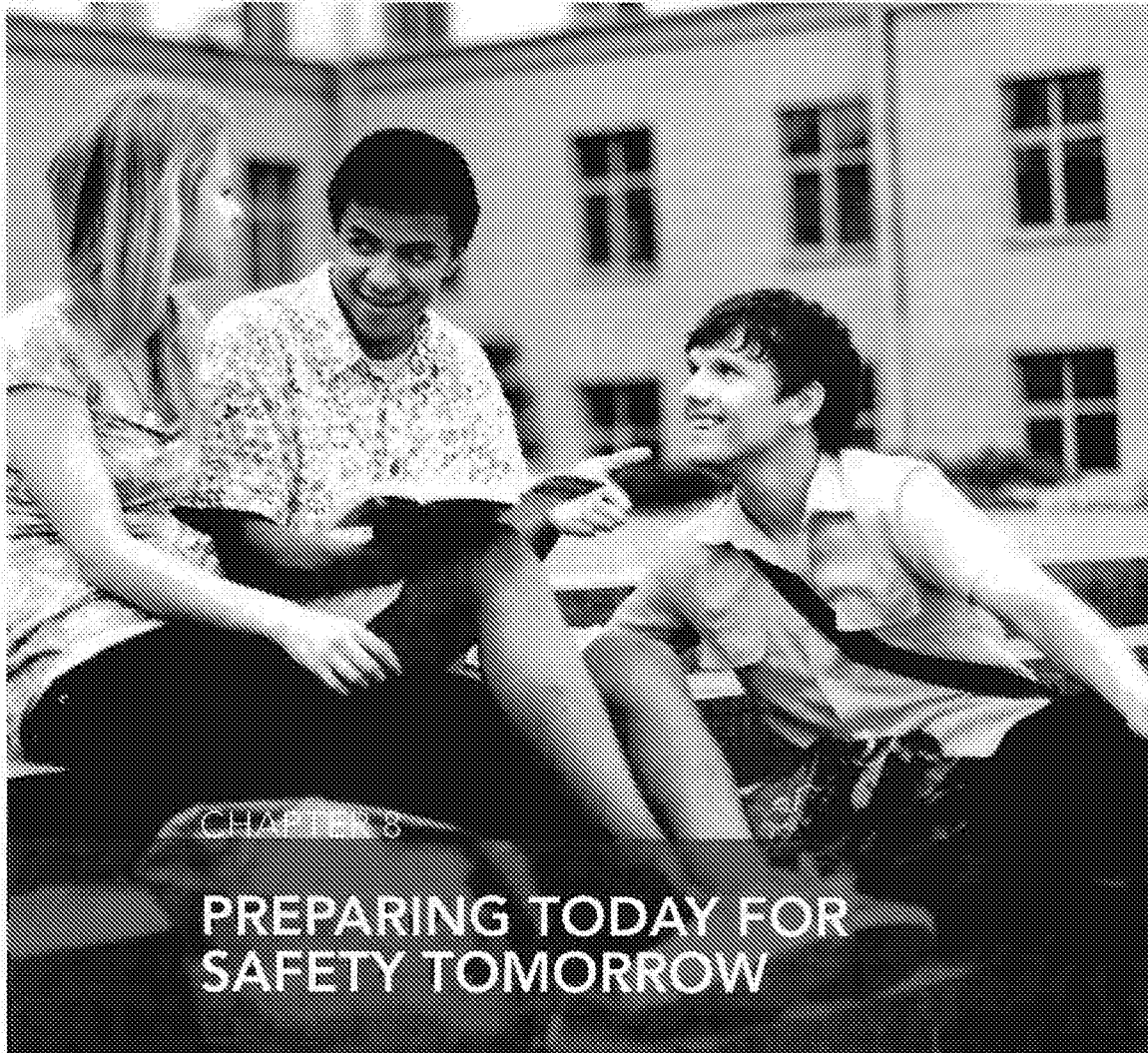
"I wish the Sandy Hook shooting never happened and very few people knew that we existed," says Quinn, whose organization saw both its membership and attendance at its annual conference decline sharply during the economic downturn that started in 2008.

"Since it did happen, we want SROs and law enforcement agencies everywhere to know what we are all about and that we're here to help."

Kevin Quinn wrote an opinion piece for CNN as part of a special series on school safety that ran in mid-January 2013. You can read it at [http://schoolsoftthought.blogs.cnn.com/2013/01/17/my-view-more-school-resource-officers-more-safe-school-communities/?hpt=hp\\_bn1](http://schoolsoftthought.blogs.cnn.com/2013/01/17/my-view-more-school-resource-officers-more-safe-school-communities/?hpt=hp_bn1).







## CHAPTER 8

# PREPARING TODAY FOR SAFETY TOMORROW

By Becky Lewis  
September 2013

### New Jersey

*The school's schedule looks like one for a pretty run-of-the-mill Wednesday. No assemblies or pep rallies, soccer games after classes (boys at home, girls away), stuffed shells for lunch.*

*The visitors walking toward the office are about to change all that. They've come from the New Jersey Department of Education's Office of School Preparedness and Emergency Planning, and in a very short time, students and staff will be called on to run an unscheduled active shooter drill.*





One of several components of a 2012 state initiative titled "Safe Schools for a Better Tomorrow (SSBT)," New Jersey's requirement for schools to participate in unannounced security drills began in January 2013. Anthony Bland, the State Coordinator and head of the Office, says that whereas many states don't require school safety drills at all, New Jersey mandates active shooter, bomb threat, non-fire evacuation and lockdown school security drills, and provides checklists and guidance on how to set up and execute them.

"Via the M.O.S.S. process, my staff also schedules visits to designated M.O.S.S. school districts to observe drills from an outsider's perspective, one drill each at elementary, middle school and secondary school levels," Bland says. "We meet with stakeholders and provide written feedback, diagnosing and prescribing just like a doctor."

Bland and his staff also provide much more to schools than just oversight to drills. The New Jersey SSBT Initiative provides direct technical assistance to schools, coordinates with local law enforcement and facilitates increased communication between school administrators and the public safety community. "We want people to know that in New Jersey we are progressive and we are doing good things."



The "good things" that make up the SSBT Initiative include, in addition to the Statewide School Security Drill Audit, Making Our Schools Safe (M.O.S.S.) Districts (which provide technical assistance), Securing Our Schools (law enforcement training), half-day school security conferences in each county, Surf's Up (Internet Safety training), symposia for nonpublic schools, ways to improve communication and surveillance infrastructure, and a upcoming model template for the state's required district-wide safety and security plan.

Bland says his office supports the initiative by providing statewide, regional and local training, and offering checklists and other supporting materials. The strength of New Jersey's efforts has impressed many, including several state representatives from Pennsylvania who have looked at possibly modeling programs on their neighbor's.

"Our state has been very aggressive in making sure that our school districts have strong guidance, and we have the potential to provide training and technical assistance to other states across the nation related to school security drills, best practices and planning," Bland says, adding it has taken New Jersey a number of years to develop and fine-tune its programs. Although the SSBT Initiative launched in early 2012, New Jersey intensified its focus on school security following the West Nickel Mines/Amish Schoolhouse shooting in 2006.





That incident, Bland says, became the impetus for convening a K-12 School Security Task Force that includes county and state officials, school administrators, school resource officers and police chiefs, and community stakeholders in developing a safe culture, all-hazards approach to address events varying from earthquakes and hurricanes to active shooter threats.

Bland says that New Jersey schools and communities have responded in a very positive way to the state's initiatives and requirements, taking pride in the knowledge they have practiced and they are prepared, but he adds: "There's no magic that will eliminate

all senseless acts of violence. People don't like to hear that, but it's true. We have great plans and great guidance, but there's no way to stop everything.

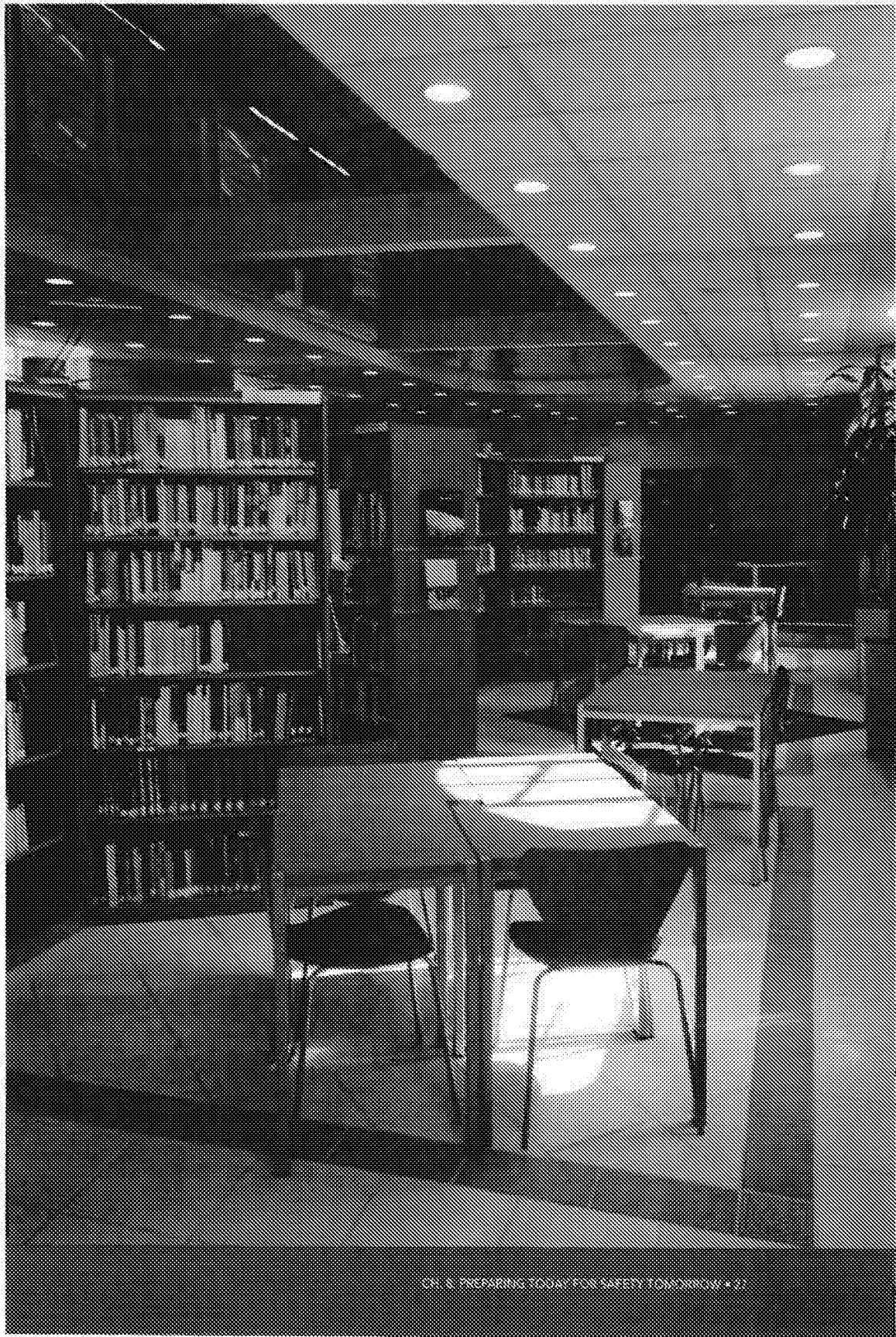
"If another state needs help with similar initiatives, we are here to help. We travel along this road together and we are a nation of one."

You can visit the following links to learn more:

- Office of School Preparedness and Emergency Planning:  
<http://www.state.nj.us/education/schools/security/>
- Safer Schools for a Better Tomorrow:  
<http://www.state.nj.us/education/schools/security/task/>
- Checklists:  
<http://www.state.nj.us/education/schools/security/task/audits/>
- Safety Plan requirements:  
<http://www.state.nj.us/education/schools/security/req/req.pdf>

Or contact Anthony Bland at (609) 584-4297 or (609) 633-6681 or email [anthony.bland@doe.state.nj.us](mailto:anthony.bland@doe.state.nj.us).









## CHAPTER 9

# VOLUNTEERS COME TOGETHER TO PRODUCE FREE TRAINING VIDEO

By Becky Lewis  
April 2013

Woodland District No. 50  
Gurnee, Ill.

*Brothers ask each other for opinions on their work all the time, starting with homework and continuing into adult life. Little did Tom Agos, Crime Prevention Technician with the Gurnee (Ill.) Police Department, know that a request to his brother for an opinion would begin the process of turning a small project for one school district into a free school safety video with a national audience.*

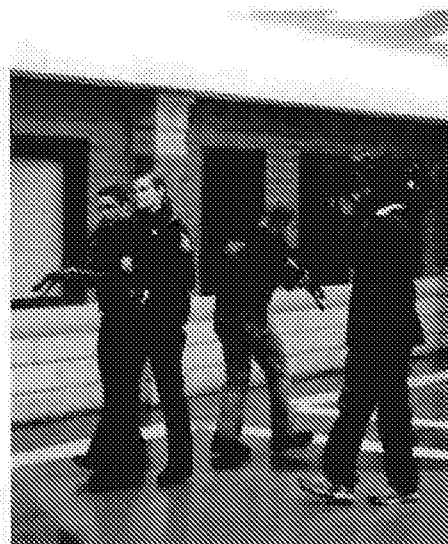




"Attention Students and Staff," a 15-minute training video, can be obtained via secure download by schools and law enforcement agencies nationwide, and Agos says the Gurnee Police Department and Woodland District No. 50 are very excited about sharing the product with other agencies – although that possibility was far from their minds when the project started. Three days after the Dec. 14, 2013, tragedy in Newtown, Conn., Agos and Gurnee School Resource Officer Jim McDermott met with Woodland's school safety team, which included district superintendent Dr. Joy Swoboda; Lori Casey, associate superintendent of education; and principals from each school building about the district's safety plan. Out of that meeting came the goal of creating a training video for substitute teachers and other support staff brought into the school system after the annual August lockdown training. Agos drafted a script and asked his brother, Chicago-area professional actor Chris Agos, for input. Chris Agos not only provided feedback on the script, he offered his services as narrator and creative consultant. Free of charge.

Another piece of the project fell into place when Agos asked Matt Till, a fellow church member and instructor for the Television Department at Columbia College Chicago (one of the largest art colleges in the United States) about the possibility of borrowing a camera to shoot the video. Through Till's efforts, Columbia College responded with donated equipment, a camera and lighting crew, student volunteers to edit video footage and compose music, and assistance, along with Chris Agos, with a casting call for officer/actors.

Tom Agos said once word got around about the project, a local salon donated hair and makeup services, a nearby restaurant provided food for the day of the shooting and "it turned from a little idea into a gigantic project with more than 60 volunteers involved. It really took off and all of the donations were a huge blessing. The result was a very professionally constructed piece that cost zero dollars to produce."

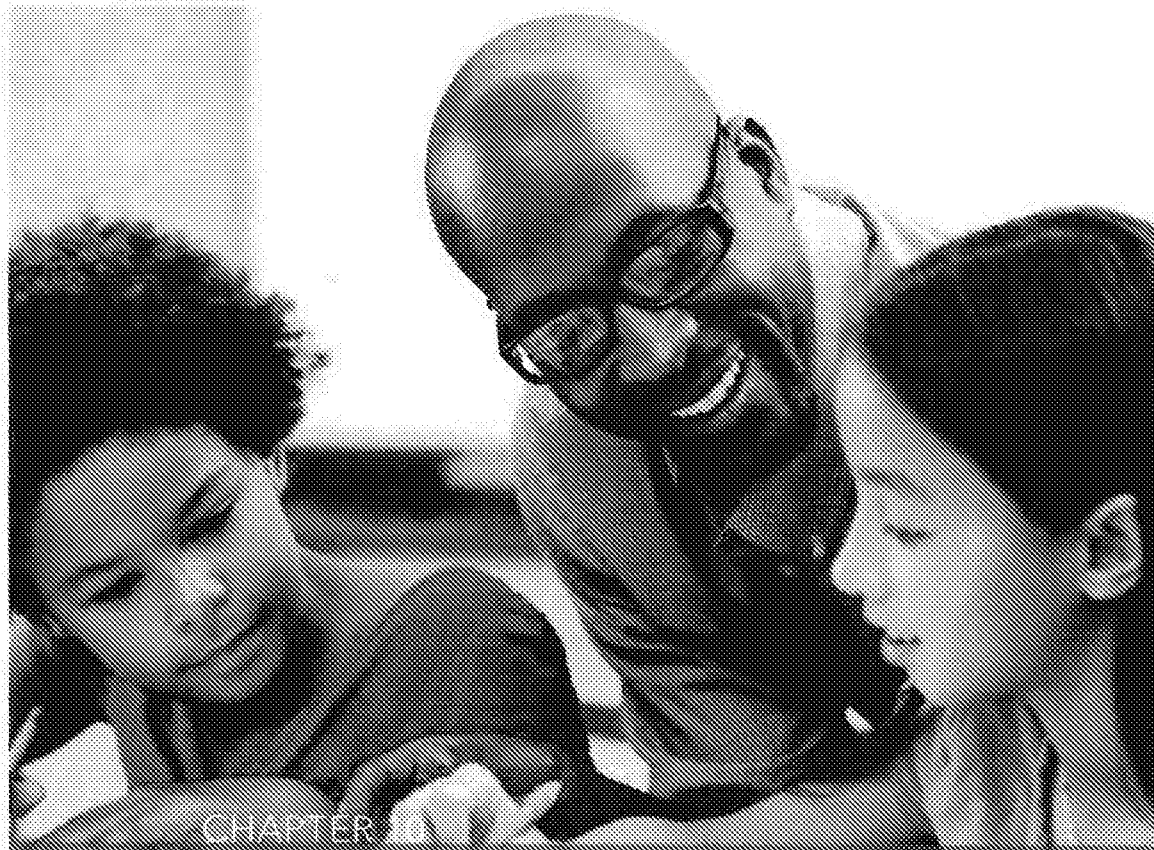


And with that came that realization that "this is just too good not to share. It's too well done and involved too much of a huge community effort to keep it to ourselves. I wrote the script so that any school district could use it if they felt it fit into their program. Other schools may have the same problem we have with hires brought in after the annual training, or for a small school district just beginning to look at school safety, it might be something they could use to build a program."

The video is not appropriate for a student or general audience, and Agos will vet all requests to ensure they come from school districts or law enforcement agencies. Qualifying entities will receive a secure link to download the video; just one week after its release, he had fielded more than 100 qualified requests.

A trailer for *Attention Students and Staff* can be viewed at <http://www.youtube.com/watch?v=iluudUhr1DA&feature=youtu.be>. To request a copy of the video, contact Tom Agos at [safetyvideo@police.gurnee.il.us](mailto:safetyvideo@police.gurnee.il.us) or call (847) 599-7080.





## CHAPTER 10

# IT TAKES A VILLAGE...

By Becky Lewis  
February 2013

### New Jersey Association of School Resource Officers

The 1996 publication of *It Takes a Village* by then first lady Hillary Rodham Clinton brought the African proverb, "it takes a village to raise a child" into public consciousness. Lt. Patrick Kissane of the Ft. Lee (N.J.) Police Department says it also takes a village to keep a child safe. Law enforcement needs to partner with other stakeholders such as school administrators, teachers and parents on school safety efforts. Kissane





uses "It Can Happen Here," a 2010 video produced by the Weapons and Protective Systems Technology Center of Excellence (WPSTC), as one tool to help promote that message.

"If you look at the SRO [school resource officer] program, it's just one piece of the pie. There are other stakeholders who need to be involved in changing the culture of a school, in preparing practice drills, in encouraging reporting," Kissane says. "The video helps bring the message to everyone that they need to be prepared."

He uses "It Can Happen Here" in presentations to principals and community leaders, and all newly hired SROs in New Jersey receive a copy to take back to their schools. (Kissane also serves as the president of the New Jersey Association of School Resource Officers and as a member of the New Jersey Governor's School Safety Task Force.)

According to Drs. Timothy Brungart and John Leathers, co-producers of "It Can Happen Here," the documentary is designed to put a face on school safety by informing and encouraging school safety stakeholders to prepare for emergencies.

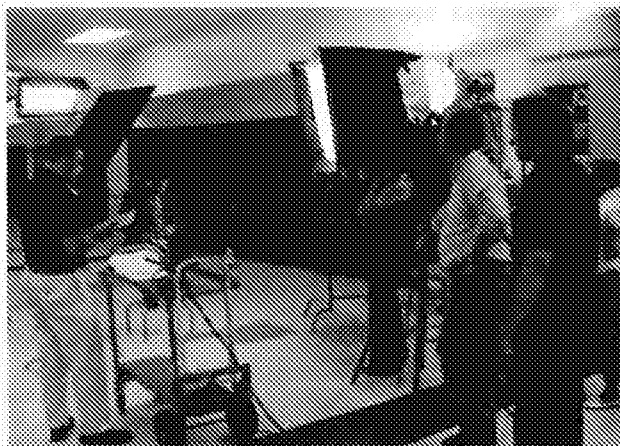
Released in 2009, the video focuses on the Columbine and Platte Canyon school shootings in Colorado and the valuable lessons that communities can learn from these tragedies.

Produced by the WPSTC for the National Institute of Justice (NIJ), the 60-minute video includes interviews with victims' parents, school administrators and local law enforcement. It also examines shootings at the West Nickel Mines Amish School, other U.S. schools and schools in other countries, and discusses technology solutions that can help law enforcement, including less-lethal technologies, metal detectors and enhanced use of surveillance cameras. In addition, the video offers a list of resources such as websites, reference materials and contacts for help with writing and implementing school safety plans.

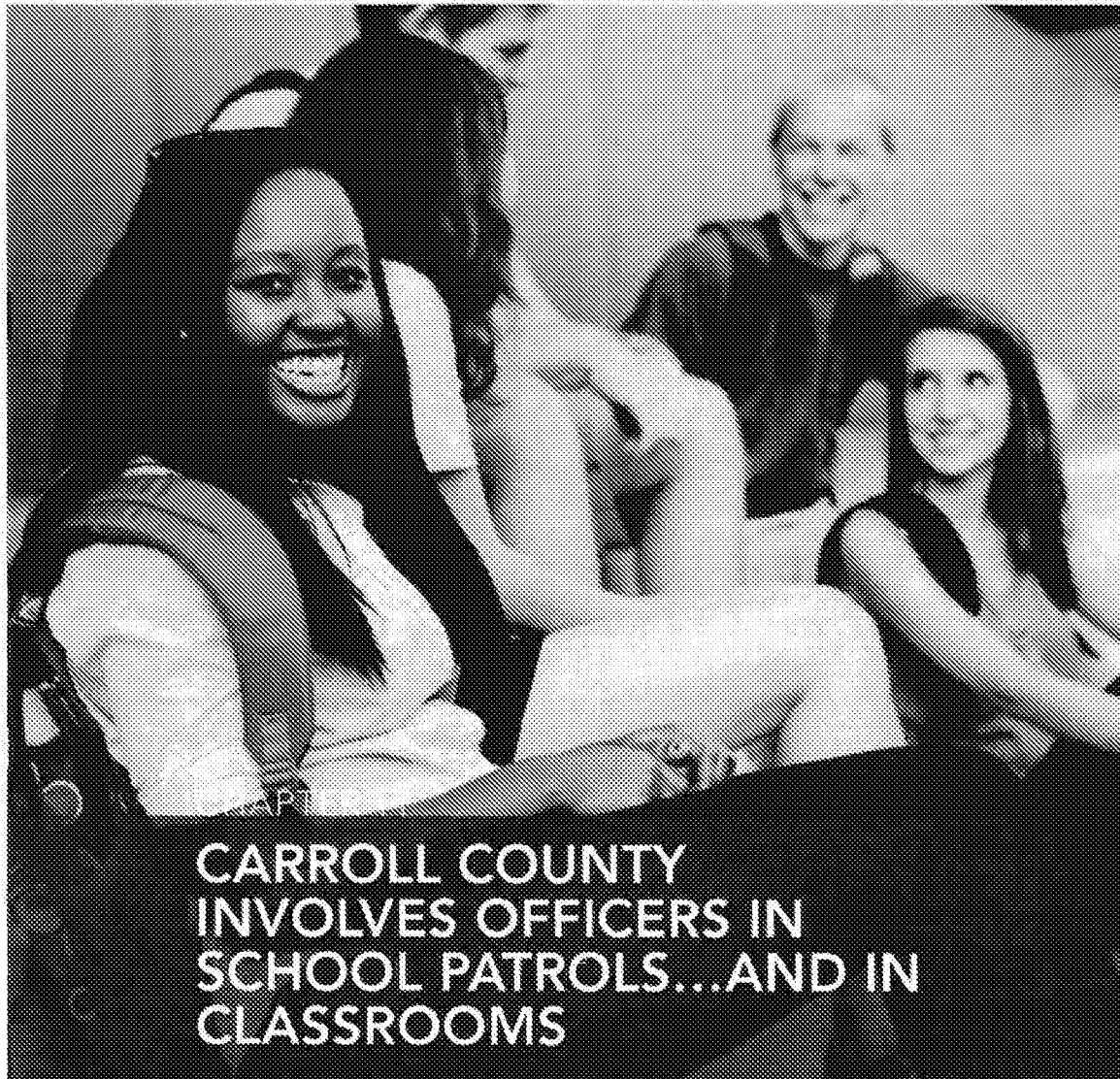
Since its release, "It Can Happen Here" has been used as supplemental material in New Jersey's mandatory 40-hour training for SROs and their chiefs, says Kissane, who served as a member of the NIJ School Safety Technology Working Group that provided subject-matter expertise during video development.

"The beauty of this tape is that the message is just as powerful and strong now, perhaps even more so, than it was when it was initially produced," Kissane says. "Around the country, everyone is consumed with school safety and they're talking about the need for more police or more armed guards, but it takes a lot more than that. It really does take a village."

For information on how to obtain copies of "It Can Happen Here," go to [https://www.justnet.org/school\\_safety.html](https://www.justnet.org/school_safety.html)







## CARROLL COUNTY INVOLVES OFFICERS IN SCHOOL PATROLS...AND IN CLASSROOMS

By Becky Lewis  
September 2013

### Carroll County, Md.

*The deputy leads the jury back to their seats. The judge calls on the foreman to stand and read the verdict: Not guilty. The judge then asks the jury members to tell why they voted not guilty, and whether they thought the defendant was not guilty when they left to begin deliberations.*





*Say what? A judge questioning jurors about how they arrived at their verdict, asking them to tell what influenced them in an open courtroom?*

*No, not a courtroom. A classroom. A classroom at Winters Mill High School in Maryland's Carroll County, where students just participated in a mock trial of a classmate charged with possession of marijuana. A mock trial orchestrated and led by two Carroll County sheriff's master deputies, co-teaching this Health I class as part of the county's new "Adopt a School Program."*

Launched with the start of the school year in August 2013, the classroom component adds another dimension to the Adopt A School program, which started with a patrol presence in the county's 44 schools following the events of December 2012 in Newtown, Conn. Officers from the county's five municipal police departments and the Maryland State Police joined sheriff's deputies in doing patrol checks and unscheduled daily visits to every school, getting to know students and teachers and offering an increased level of security.



Larry Faries, the school system's coordinator of security, explains that despite its nearness to the Washington-Baltimore metropolitan area, Carroll County remains relatively rural, with just more than 100 patrol officers (out of 214 sworn officers).

"We didn't have the resources to hire school resource officers, and we think we came up with something unique that gives us a lot of 'bang for our buck,'" Faries says. "Every patrol officer is involved in security instead of just a few. They stop in and eat their lunches, they take in their laptops and file reports, they walk through the school and get to know everyone there."

Although the patrol component started almost immediately after the shootings at Sandy Hook Elementary, working out the teaching component took some brainstorming and planning over the course of several months. Dawn Rathgeber, assistant supervisor of Curriculum and Instructional Resources, and Chief Deputy Phil Kasten led the team that developed the teaching component.

"We agreed that DARE had been a good thing for the county, and we didn't want to lose that instructional component but we wanted to build on the DARE experience. We came up with this idea to include foot patrols and being visible around the campus, yet still getting to know the kids and develop relationships with them in the classrooms," Rathgeber says. "I'm so pleased the classroom interaction will continue. Police officers are people too and we didn't want to lose the foundation we already laid."

Whereas DARE presents a structured 10-day, in-and-out of the classroom component, the Adopt a School curriculum features officers co-teaching several dif-





ferent units with a certified health teacher, including the dynamics of emergency, bike safety, "stranger danger," the legal consequences of underage alcohol use and drug use, strategies for dealing with peer pressure, cyber-bullying and on-line safety. Collaborative instruction takes place throughout the school system, as students in the second, fifth, seventh and eighth grades participate along with students enrolled in secondary school Health I. Carroll County has trained 20 officers from the various law enforcement agencies, with those from municipal agencies teaching in their towns, and sheriff's deputies and state troopers teaching at the other schools.

"We did an interview process and selected people based on their ability to give a presentation as well as their written and oral communication skills. They went through a one-day training before the school year, working with instructional staff from the schools," says Kasten. "We think that adding the officer to the teaching team gives them the chance to enhance the lessons based on their experience."

Two of the officers selected, Master Deputy Worthington Washington and Master Deputy Jeremy Holland, worked with health teacher Salvatore Picataggi to create the mock trial that drew avid participation from Winters Mill students. Washington, a veteran of the DARE program, calls Adopt a School a good partnership that gets students used to seeing officers in class and "lets them get to know us as people and not just officers. By interacting with them, they can feel comfortable coming to us if they need our help as officers. The teachers like us coming in too."



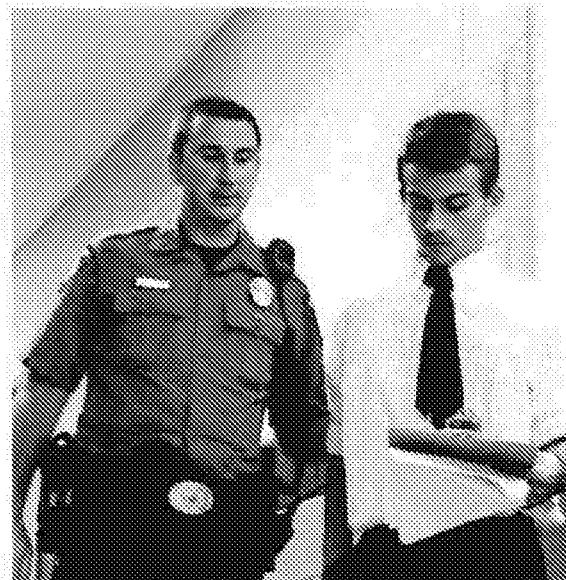
And Holland, who became interested in working in a school system due to a positive relationship as a student with the SRO at Franklin High in suburban Baltimore (Reisterstown), says he feels very optimistic about what's going on in Carroll County: "I feel very optimistic about the program. I hope that each of these kids, from my being here, will make the right choices when they're faced with them."

Sheriff Ken Tregoning shares Holland's optimism, and in addition, calls the Adopt a School program a very innovative one: "We're applying more resources into the schools and we're improving physical security inside and outside the schools. We're using more deputies and police officers to make sure our schools are secure. There's a visibility and a presence, and they also interact with the students on a personal basis. It brings law enforcement, school administrators and students closer together."

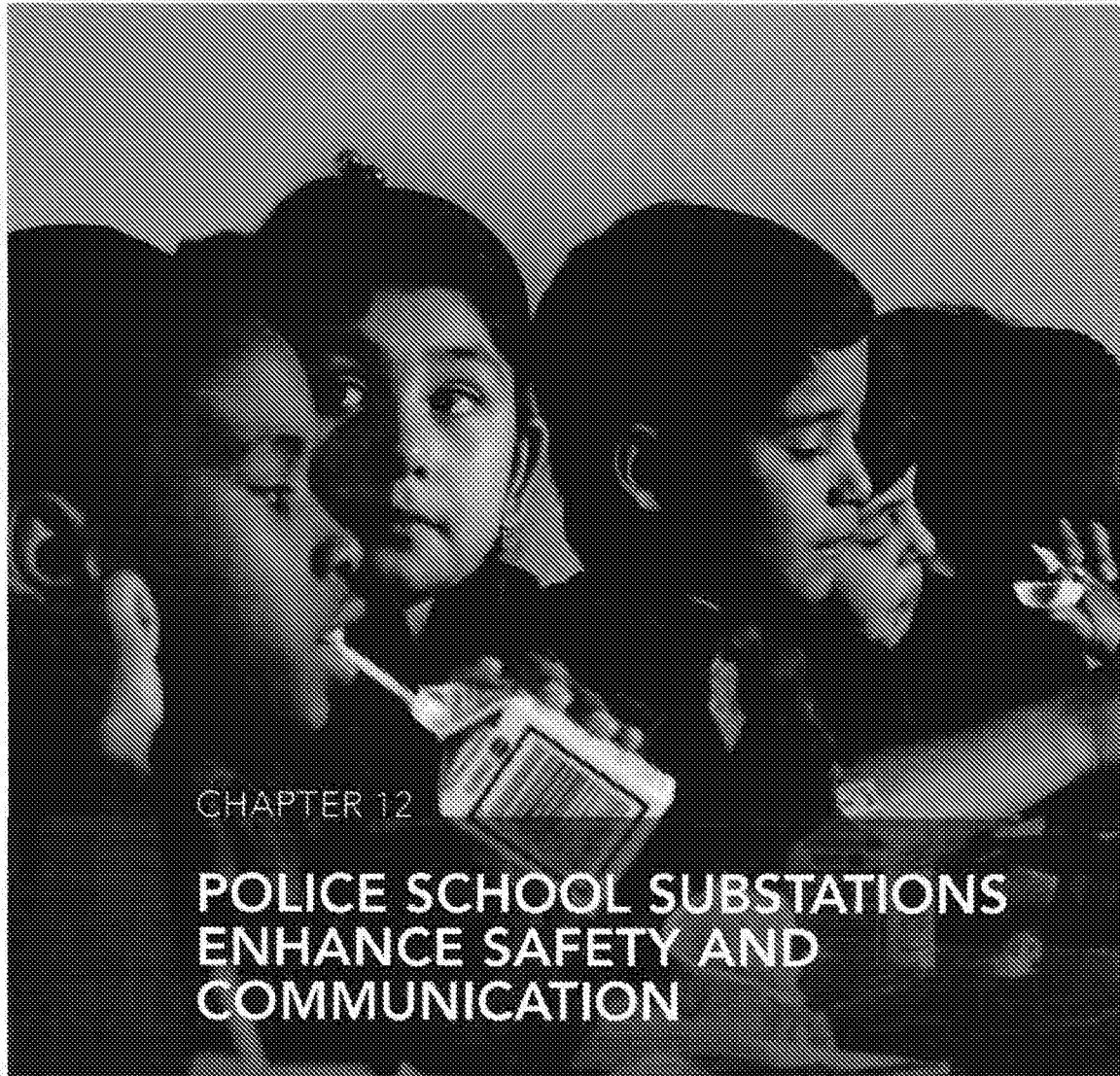
Carroll County Superintendent of Schools Stephen H. Guthrie echoes his sentiments about providing visibility along with the educational components, "and the administrators know a familiar face, and they know they have a person to call who knows the history of the school and knows the students. I also don't want another school district that might want to do the same thing to think this all came together out of the blue. It was fostered in more than a decade of good relationships between Larry [Faries] and local law enforcement, that's why it came together so easily and quickly. To replicate it would require a lot of groundwork."

*For more information on Carroll County's Adopt A School program, contact Larry Faries at (410) 751-3171 or email [lefaries@carrollk12.org](mailto:lefaries@carrollk12.org), or Dawn Rathgeber at (410) 386-1687 or email [gd Rathg@carrollk12.org](mailto:gd Rathg@carrollk12.org).*

*Also, a more detailed article and accompanying video can be found on JUSTNET, the website of the National Law Enforcement and Corrections Technology Center system.*







## CHAPTER 12

# POLICE SCHOOL SUBSTATIONS ENHANCE SAFETY AND COMMUNICATION

By Michele Goppola  
March 2013

### Elementary Schools Goodyear, Ariz.

*Young students were thrilled to have lunch with a police officer the other day. But then, that's become an almost routine occurrence at several elementary schools in Goodyear, Ariz.*





Police and school officials in Goodyear, Ariz., have set up police substations in three elementary schools, increasing police visibility and fostering communication between law enforcement and the school community.

Under the program, officers stop by the schools during the day and use office space provided by the schools to do paperwork or make phone calls during their shifts. Officers are not assigned to a school or required to go to a school. Their schedules and duties on any given day determine when they can drop in and use the office.

"It's a great opportunity to have police visibility on campus," says Lisa Kutis, police public information officer. "Having police officers on campus acts as a deterrent to crime. It also paints officers as positive role models, and some officers enjoy stopping in during lunch time and interacting with students. The program is also fiscally responsible because there are no out-of-pocket costs to the school district or the police department."

Gina DeCoste, principal of Mabel Padgett Elementary School (825 students), proposed that police set up a substation at her school following the school shootings in Newtown, Conn., in December 2012. The program began in early January at Mabel Padgett, and expanded to two more elementary schools, Westar Elementary and Centerra Mirage School, later in winter 2013.

"The kids love it, they think it's really cool having a police officer on campus," DeCoste says. "Usually the officers take a walk around and see the kids because the kids get so excited, and the parent feedback has been extremely positive."

"Having officers on campus provides a positive role model for students and peace of mind for parents and staff. In addition, the police car parked outside adds a visual deterrent to someone wanting to commit a crime."

The school already had a working relationship with the police department, and the substation has furthered that bond. Police participate on the school's safety committee.

"We are building relationships, and when issues come up where we want law enforcement advice, it's nice that I can walk down the hall and say 'can I run this by you real quick?' " DeCoste says. "We had the foundation for a good working relationship with Goodyear PD, and I believe that has helped make the substation successful."

The Goodyear Police Department, with 94 sworn officers, serves a population of about 66,000 residents and is a suburb of Phoenix. The substations are located in three separate geographic areas of the city — the north, south and central areas of Goodyear — and encompass three separate school districts, all located in Goodyear. Full-time school resource officers serve the city's high schools and are available to respond to other schools if needed.

"The substations foster better communication with school staff and the student body, and a fully marked police car outside increases visibility and awareness of police in the community," says Lt. Scott Benson of the Goodyear Police Department. "The students are great and we get very positive feedback. They find us approachable and it gives them a better understanding of police. It gives them an opportunity to see us in a different light."

For more information, contact Lisa Kutis at (623) 882-7663 or [lkutis@goodyearaz.gov](mailto:lkutis@goodyearaz.gov).





## CHAPTER 13

# POLICE OUTFITTED WITH MASS CASUALTY TRAUMA KITS

By Michele Coppola  
February 2013

**Tucson Police Department  
Tucson, Ariz.**

*Kneeling at the side of the gunshot victim, his co-worker calls out to the responding police officer that "he needs help right away, where's EMS?" The officer knows just what to do: get the emergency kit from his vehicle and do what he can to stabilize the victim until emergency medical services can safely enter the scene.*





The Tucson Police Department can use its advanced emergency medical kits to provide first aid to victims of a mass casualty incident before emergency medical personnel arrive. The kits are designed to effectively allow police officers to render first aid and life support on the scene of a mass casualty incident similar to what occurred at Sandy Hook Elementary School or the attack on Congresswoman Gabrielle Giffords, her staff and community members. They compress the time it takes to stabilize injuries before paramedics arrive, according to Capt. David Azuelo, Commander, Emergency Management and Homeland Security Division, Tucson Police Department.

An interim solution for patient care is necessary because paramedics will not typically enter a scene until police have located and stopped the threat(s), actions that often can take a considerable amount of time given the complexity of these incidents as well as the varying and contrasting information that is often prevalent at the onset of an active shooter type of situation.

"Many times fire agencies will not come into a 'hot zone' so it is up to law enforcement to not only deal with the threat, but also provide stabilizing first aid to survivors until they can be transitioned to paramedics," Azuelo says. "The mass casualty trauma kits allow officers to bridge the gap by providing immediate first aid during what is often referred to as 'the golden hour,' the timeframe that is most critical to patients suffering from traumatic penetrating injuries. It gives a police officer without a tremendous amount of training in advanced medicine the ability to save lives."

"We recognize that a mass casualty shooting event is likely going to be one of the most difficult calls a police officer ever responds to, not just in terms of dealing with the threat, as that is something most officers are well prepared for," he adds. "Rendering aid in a timely manner to numerous severely injured victims is not something most officers deal with on a regular basis, therefore we recognized from a management perspective that we needed to ensure these kits were useful, relevant, and not overly complicated for police officers to use. We wanted a patrol-ready, easy-to-use, mass casualty trauma kit that would meet the needs of all of the primary injuries you would find in a mass casualty situation."

Recognizing the need to bridge the gap of time it takes for police officers to transition patients to advanced life support care during an active shooter event, Paramedic Capt. Kristopher Blume, also a tactical medic and the manager of the Metropolitan Medical Response System in Tucson, collaborated with the TSSI company to develop the mass casualty trauma kits for the police department.

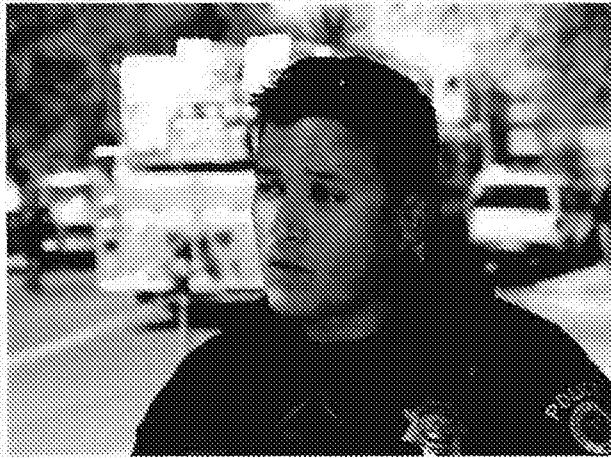








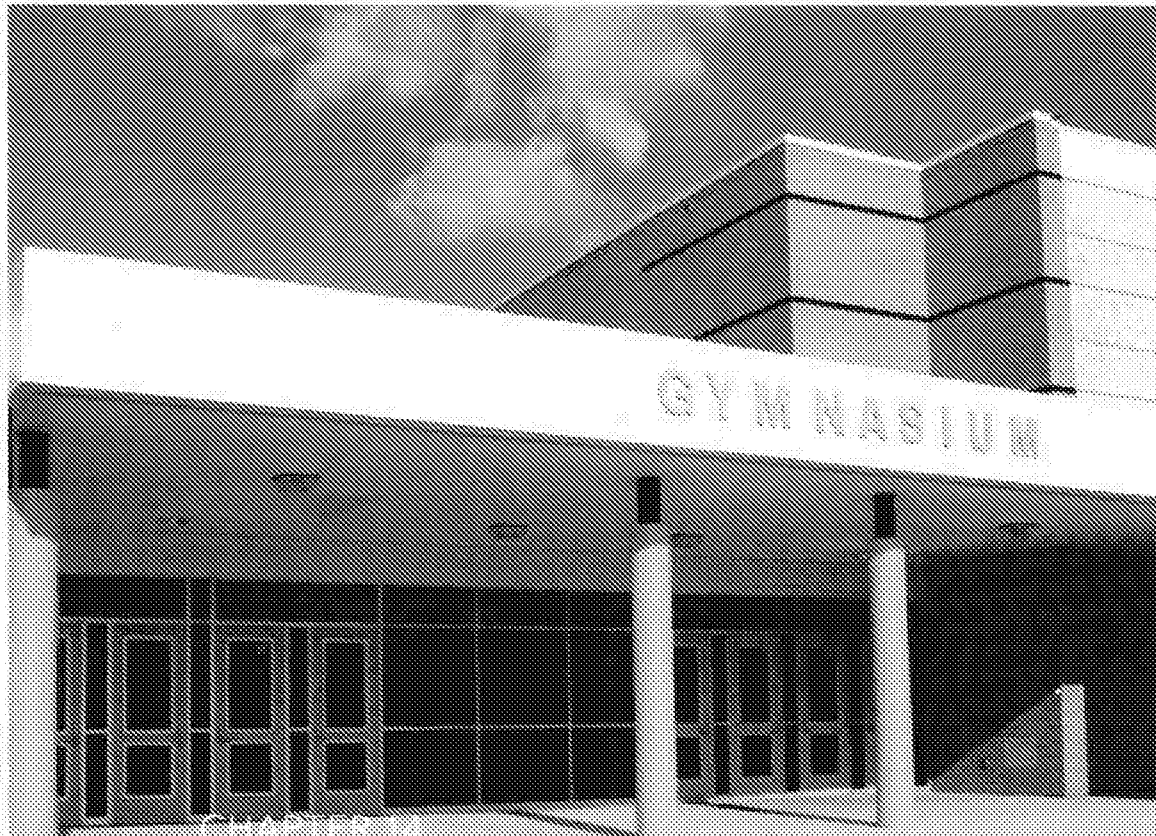
The packs, which fit in the trunk of a police sedan, consist of a large nylon case that contains six individual advanced first aid kits, along with additional splints, bandages and trauma blankets. Tucson has eight packs, which cost approximately \$3,000 each and were purchased with funds from the U.S. Department of Homeland Security Metropolitan Medical Response System grant program (now defunded). The packs have been distributed to each of the department's five patrol divisions and to members of the full-time Special Weapons and Tactics Team. Every officer is certified in basic first aid but the police department is working with the fire department to further refine training specific to the mass casualty trauma kits."



"The packs are the result of awareness of the totality of what was occurring around the nation," Azuelo says. "Mass casualty incidents are nothing new. These types of situations have occurred for decades. Law enforcement has a different mission than fire and paramedics, but we have recognized that we have to come together better because in certain situations, unless we can provide aid to those victims, the likelihood of their surviving long enough to get them to paramedics is slim. We need to respond as quickly as we can to get them to paramedics and ultimately to the hospitals."

*For more information, contact Capt. David Azuelo at (520) 837-7378 or [david.azuelo@tucsonaz.gov](mailto:david.azuelo@tucsonaz.gov).*





CHAPTER 24

## IN-DEPTH SAFETY AUDITS EXPAND SCHOOL SECURITY

By Michele Ceppola  
July 2013

Albemarle County  
Virginia

*Landscaping. Check. Lighting. Check. Points of entry.  
Check. Parking areas. Check.*

*All these areas and more come under review during a Crime Prevention Through  
Environmental Design (CPTED) audit.*





Police in Virginia's Albemarle County are performing extensive safety audits on all public schools as part of an effort to expand school security. Officer Steve Watson, a crime prevention specialist with the police department, explains that the county's school resource officers periodically performed safety audits in the past, but the county wanted a more in-depth process.

Three officers from the Albemarle County Police Department attended a course in spring 2013 based on Crime Prevention Through Environmental Design (CPTED) principles. On completion of the three-day course, which is offered through the National Association of School Resource Officers (NASRO), participants are certified as NASRO school CPTED practitioners.

"The schools worked with us to try and get the schools a little safer. It was an evolved, concerted effort," Watson says.

The class the Albemarle officers attended in Kansas was the first NASRO school CPTED certification class held. According to the course description, CPTED "uses design, management and activity strategies to reduce opportunities for crime to occur, to reduce fear and to improve overall safety of schools. The CPTED concept emphasizes the relationship of the physical environment, the productive use of space and the behavior of people." The course includes a hands-on evaluation of a school and provides attendees with tools to use on their school campus.



As part of their school inspections, Albemarle officers use a lengthy survey form provided by the Centers for Disease Control and Prevention (CDC) to review the interior and exterior of the building and examine numerous aspects of school security. The audit looks at organizational structure, mechanical aspects and crime prevention techniques such as locks and surveillance cameras.

"We use the CDC form every time we do a school audit. Basically we are looking at the interior and exterior of the school," Watson says. "CPTED is about how to use the natural environment to create a safer school — proper landscaping, proper lighting, how to bring people into the entrance without problems and creating areas that discourage potential criminal activity. We are looking at how to manipulate the environment to make it safer."

Officers consider numerous security issues when evaluating a school.

"My main thing is to look at access, who has access and who is it controlled by," Watson says. "When people are inside are they identified with visitor badges? Can people get in without going through the main entrance?"





"Basically we take an initial impression when we arrive," he adds. "We look at the perimeter and how boundaries are defined, is the school easily seen, points of entry, main entrances, exterior of the building, and drop-off and pick-up areas. We look at parking areas, whether visitor parking and staff parking areas are separate and are they monitored by cameras. We look at pedestrian flow through the school property, whether it is monitored and can it be monitored better. We consider all learning buildings, including trailers and whether they are safe,

locked, and well-lit, and whether the building doors get propped open during the day."

Police also look at the cafeteria and the interior office and whether there is good surveillance of the lobby area. They look at restrooms and the overall picture of how students can stay safe with other students.

"The review is pretty extensive. It's a little bit of everything," Watson says.

The county has 26 public schools. Police began their school audits in June 2013 and planned to complete most elementary school audits in 2013 and begin reviewing middle and high schools in 2014. The following year they would like to begin doing reviews of the schools they have already completed.

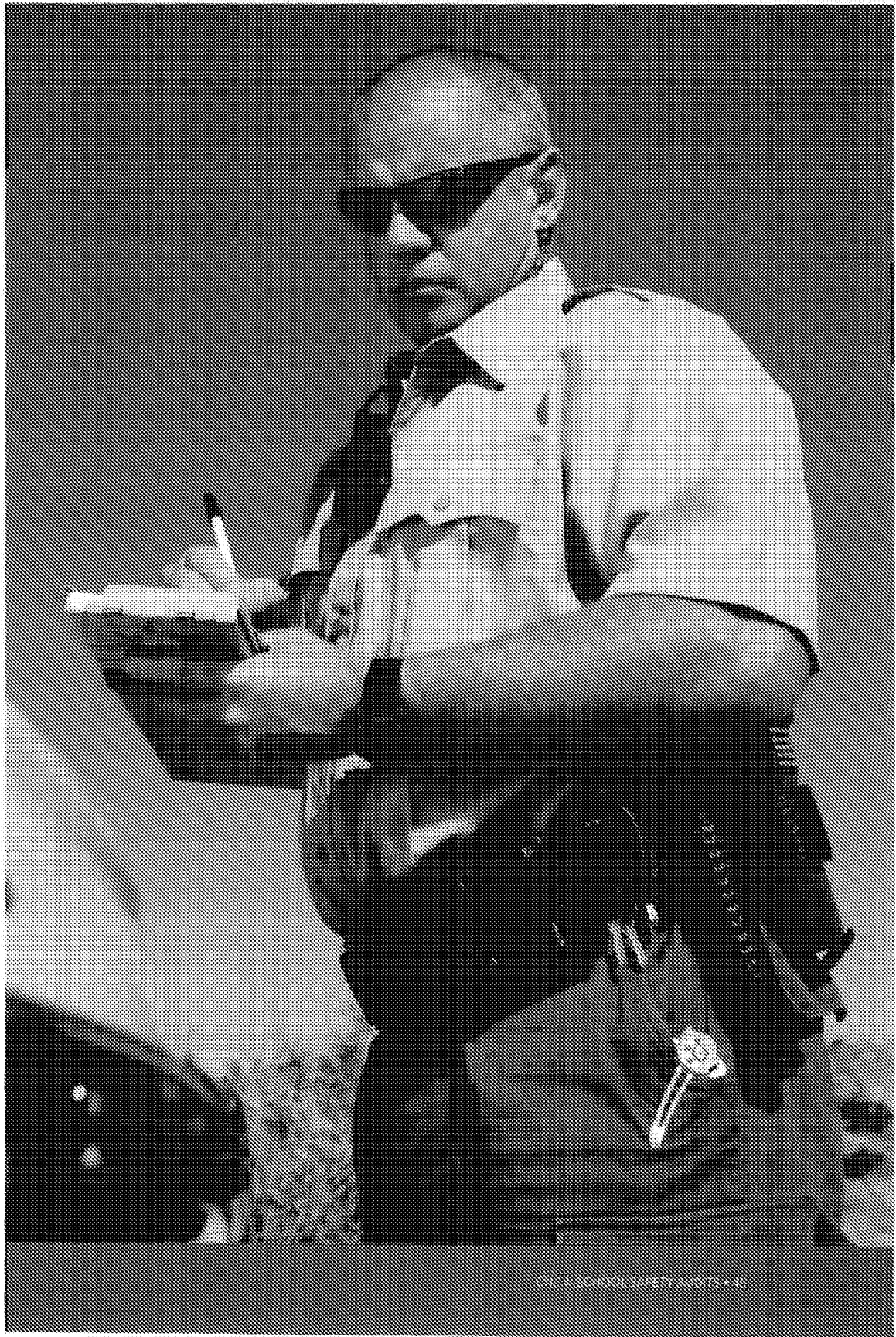
"My goal is to have a yearly process and meet with administrators and see if there are additional safety concerns. Our main goal is to make it a continual process," Watson says.

Each audit takes between 30 and 60 hours to complete. Officers present their findings and security recommendations to school administrators, including guidance on how to understand the 30-page CDC form ratings and photographs of the schools to understand safety redesign recommendations.

"The goal of the training is to have officers get those tools to take them back to schools and communities and evaluate their campuses through the CPTED principles to try to make the schools a safer place," says NASRO president Kevin Quinn, who is a school resource officer in Arizona. For more information on NASRO, see "The Immediate First Responder" on p. 22.

*For more information, contact Officer Steve Watson of the Albemarle County Police at [watsons@albemarle.org](mailto:watson@albemarle.org). To learn more about the NASRO school CPTED course, go to <http://www.nasro.org/content/school-cpted-practitioner-certification>.*









## CHAPTER 15

# SCHOOL CRITICAL INCIDENT PLANNING – GENERATOR (SCIP-G) HELPS CREATE COORDINATED RESPONSE

By Becky Lewis  
February 2013

### Sumter County Police Department South Carolina

Although the administrators at the Sumter (S.C.) Police Department fervently hope they never have to deal with an active shooter situation, they want to have Incident Command System (ICS) plans in place for every one of the county's 30-plus schools in case such an event does occur. Emergency Management Coordinator Gary Fowler has





*found that the National Institute of Justice (NIJ) School Critical Incident Planning – Generator (SCIP-G) is the right tool to help with that process.*

"We wanted to establish an ICS plan that will work so that we don't have to come up with one on the fly in the event of an emergency," Fowler says. "We know which specific people need to be in specific positions. We know exactly what we need to do. I've been working a lot with SCIP-G so that we don't have to reinvent the wheel. I'm able to use it to look at each school at the incident command level and determine what we need to do to coordinate our response with school administrators."

SCIP-G provides step-by-step guidance for creating a plan, using the most widely accepted law enforcement practices and procedures as the foundation. It can be found on NIJ's Triple Play School Safety Combo CD, which also includes "A Critical Incident: What to Do in the First 20 Minutes" and "School Crime Operations Package (School COP)."

"My chief asked me to work up our intended response protocol in dealing with an active shooter," Fowler says. "We're looking at the immediate armed response, and we train on different aspects of that, such as whether it's a hostage situation or whether there is an active shooter inside a school. And we could extrapolate from this training as needed to apply to a workplace violence incident at a business."



Sumter PD plans to involve the other law enforcement agencies in the county — the Sumter County Sheriff's Office, South Carolina Law Enforcement Division and Department of Natural Resources Police — in the planning and training. In addition to using SCIP-G, Sumter PD is in the process of conducting site surveys and taking pictures of every school. Computerized floor plans will designate command posts and which officers will be stationed where.

Fowler says he is also sending letters to every school, asking administrators to designate a point of contact who will work with law enforcement on developing the plan and then be accessible in the event of an emergency. The agency is reaching out to the county's public and private schools, which range from small rural schools to larger ones in the more urban Sumter city area (population 42,000 of the county's 108,000 residents), and include a University of South Carolina branch campus.

"We've been working on this for several years. We've had training in the past, and every year we go through refresher courses," Fowler says. "However, this is the first time we are undertaking an effort to put everything on record so that the appropriate people know exactly what their specific duties are."

You can download the Triple Play combo from <http://srtbrc.org/downloads/> or order it by mail at <http://srtbrc.org/form/view.php?id=9>.





CHAPTER 16

## SMARTPHONE APP PROVIDES ALTERNATIVE WAY FOR STUDENTS TO COMMUNICATE WITH POLICE

By Michele Coppola  
February 2013

Anne Arundel County  
Police Department  
Maryland

*Students in Anne Arundel County, Md., schools can now use a familiar, comfortable way of reporting bullying or other problems to police: an app.*





The Anne Arundel County Police Department released the free AACo PD Speak Out app in fall 2012. The School Resource Unit designed the app to provide students with a way to communicate in a secure, private fashion. Students can walk into the office of a school resource officer (SRO) or use a phone tip line to report a problem, but police wanted to ensure students had another option to encourage communication.

"We are trying to put more tools in kids' hands in an environment they are used to working with," explains Lt. Doyle Batten, school safety section commander for the department. "We wanted to give kids as much anonymity as possible to let us know what is going on."

The county's 125 schools serve approximately 78,000 students. SROs are present in all 12 of the county's high schools and are authorized for 11 of the county's 19 middle schools.

The app is available through the Internet at <http://aacopdspeakout.myapp.name> or through the Google Playstore for Android products or via iTunes for iPhone users. Although the app is designed for public school students in the county, a parent or a private school student can use it as well. Police forward the email message content to where it needs to go, such as a specific school or SRO.



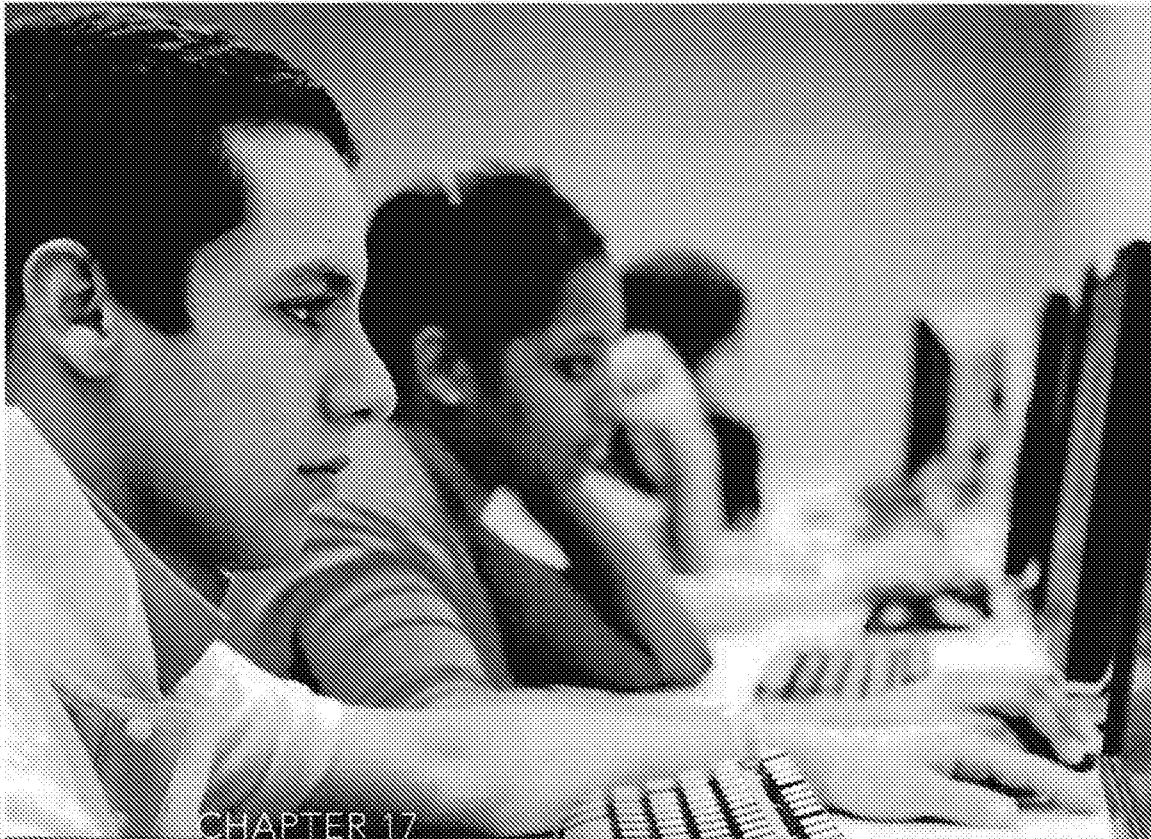
"Through all of our research, we can't find any other police SRO agency that has tried this," Batten says. "We are interested in seeing what direction this takes. We don't know how it might morph over time. We definitely see it as an avenue for identifying bullying and gang activity."

There have been several successful uses of the app thus far, according to Batten, involving students in emotional distress and bullying.

"None of these were major incidents, which is exactly how we hoped it would go — intervention at an early level," Batten says. "Information is the key to prevention."

For more information, contact Lt. Doyle Batten at [dbatten@aacounty.org](mailto:dbatten@aacounty.org), (410) 222-0040.





## CHAPTER 17

# ANONYMOUS REPORTING AND PREVENTION PLATFORM HELPS STOP TROUBLE BEFORE IT STARTS

By Becky Lewis  
August 2013

Thomas Nelson Community College, Va.  
Tulsa (Okla.) Public Schools

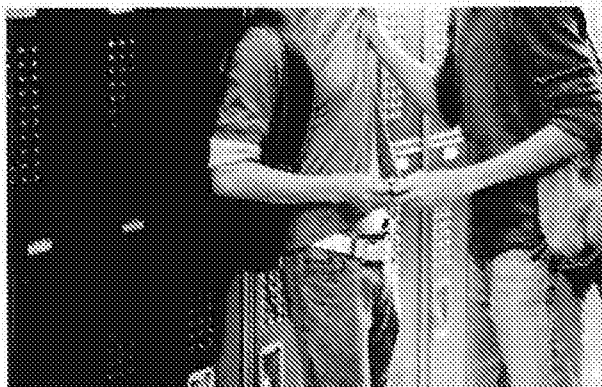
*The accounts show a disturbing similarity: three separate reports over a period of 24 hours have come through the anonymous "hot button" on the school's website, all expressing concern about suicidal tendencies by the same student. Reports that will lead to a successful intervention and possibly, a life saved.*





The Safe School Initiative, a project of the U.S. Secret Service and the U.S. Department of Education ([http://www.secretservice.gov/ntac\\_ssi.shtml](http://www.secretservice.gov/ntac_ssi.shtml)), encourages schools to emphasize focusing on possible warning signs in student behavior, and to encourage students and faculty to pass along concerns instead of dismissing them as “it’s probably nothing.” However, particularly among students, there is fear that reporting their concerns may make them a target, or they may get into trouble themselves if their suspicions prove unfounded. One answer may be an anonymous reporting system, one that allows students – and also faculty, staff and others – to confidentially express those concerns.

As part of an existing Virginia state contract, Thomas Nelson Community College (TNCC) recently took the lead among 20 schools in the Virginia Community College System and began using an anonymous reporting and prevention platform, joining secondary schools and institutions of higher learning across 13 U.S. states and Canada as innovators looking to improve student safety. And halfway across the country in Tulsa, the public school system has used the same prevention tool for nearly two full school years.



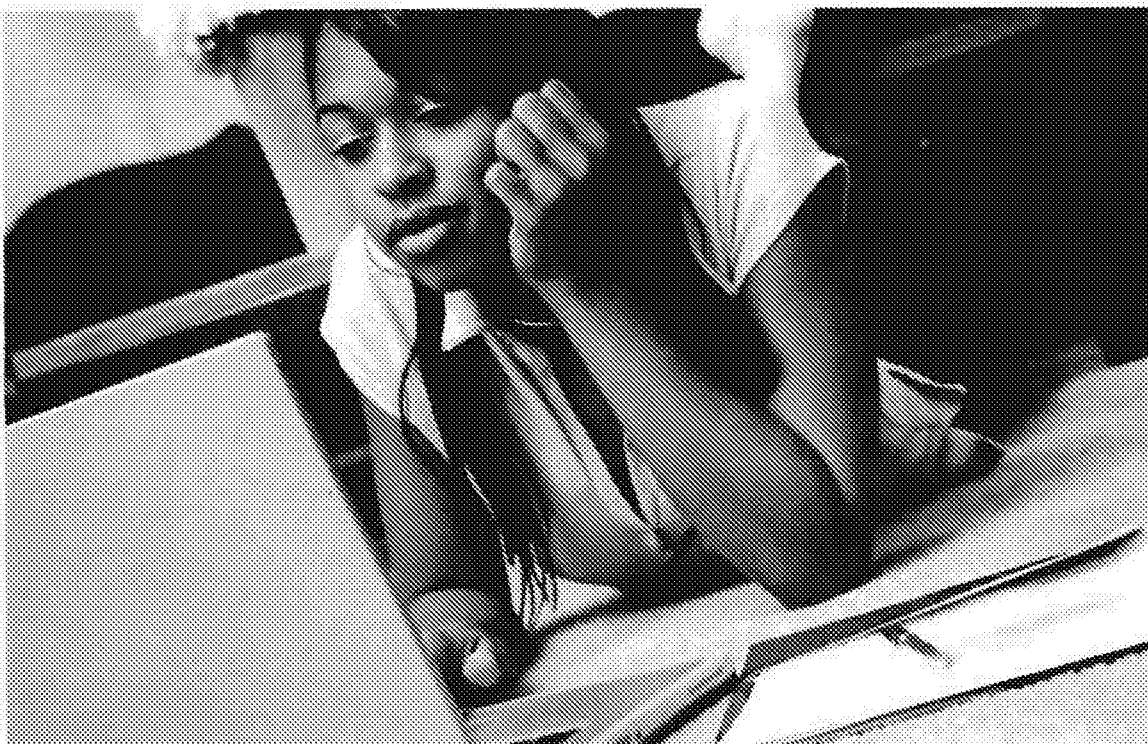
Both campuses have already achieved positive results and used the innovative web-based platform to prevent potential incidents.

Garth MacDonald, Emergency Management/Campus Safety Manager at TNCC, says when he took that job in March 2011, it was with the understanding that looking at how the college of 16,000-plus students captured reports of potential issues and problems was a top priority. He determined that the existing in-house reporting system seemed cumbersome and difficult to access from devices such as tablets and smartphones; also, only the individual who first looked at a report had access to the information.

“I did some research and realized the company that did our online training for computer security also offered a software program for reporting activity and threats. We decided that was the right route to follow, and it has proven itself a very versatile tool. When a report comes in, all team members receive a simultaneous notification, and any comments made are shared with all team members,” he says. “The system allows the person making the report to upload pictures, so individuals can use their phones to back up their statements with photos.”

Tenna Whitsel, student services coordinator with Tulsa Public Schools, described a similar research process, this one driven by a steering committee looking at how to address ongoing issues with bullying: “We learned that best practices recommended anonymous reporting, and we knew that students already have a problem with trust and don’t want to tell anyway. We knew we needed something more than a shoebox with the words “Anonymous Reporting Here.”





Her research led her to a webinar promoting a software package that she instantly knew was the right product for Tulsa, and the “hot button” to the reporting form went up on the district’s website in January 2011. Gary Rudick, campus police chief, says that although Tulsa initially focused on bullying, reports to the system cover a number of other issues, including students bringing firearms to school, threatened assault and dealing drugs. Those reports can prove a great asset to a 23-member police department charged with oversight of more than 40,000 students and 7,000 employees at more than 100 different sites. Rudick says the campus police review every report to determine if a criminal act has been committed rather than waiting for someone to come forward to file a formal complaint.

Whitsel adds that the system also provides oversight response to handling of allegations, holding administrators, employees and law enforcement accountable for followup: “One thing students really like is they get to enter a complaint through our website just like an adult, instead of having to come in and tell someone ‘They’re picking on me.’ It empowers them and makes them feel like they did something about it, which is a benefit that I didn’t anticipate.”

Just like in Tulsa, the nine-member TNCC team has also received a wide range of report types, covering everything from assault to suicidal gestures. If the emergency management team perceives an immediate danger, the information is passed on to campus police. Otherwise, team members do some legwork to ensure the allegation is valid and determine the best course of mitigating action:



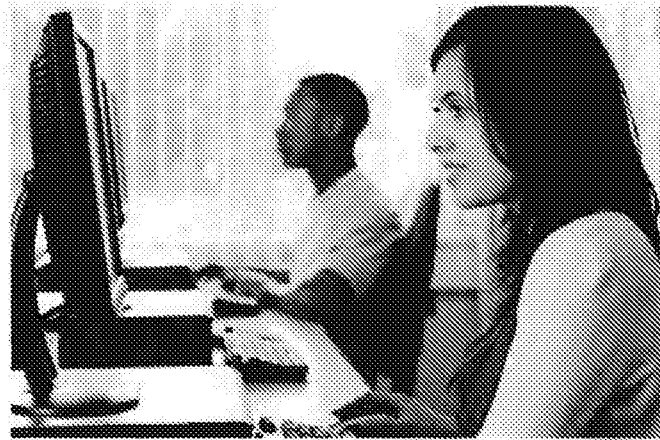
"That's the basic goal, to prevent someone from becoming a casualty at their own hands, or, God forbid, coming onto the campus as an active shooter."

Rudick says that "basic goal" has already been reached in Tulsa, where a tip led police to prevent a potential active shooter incident. Other tips have helped officers stop fights before they happen and intervene in drug deals. And the system has cross-checking capability that links reports about the same individual, even if they take place weeks or months apart, which allows schools to reopen cases if needed. Those cross checks, along with reporting features, help lead to the accountability that Whitsei emphasized as important, and is important to MacDonald as well.

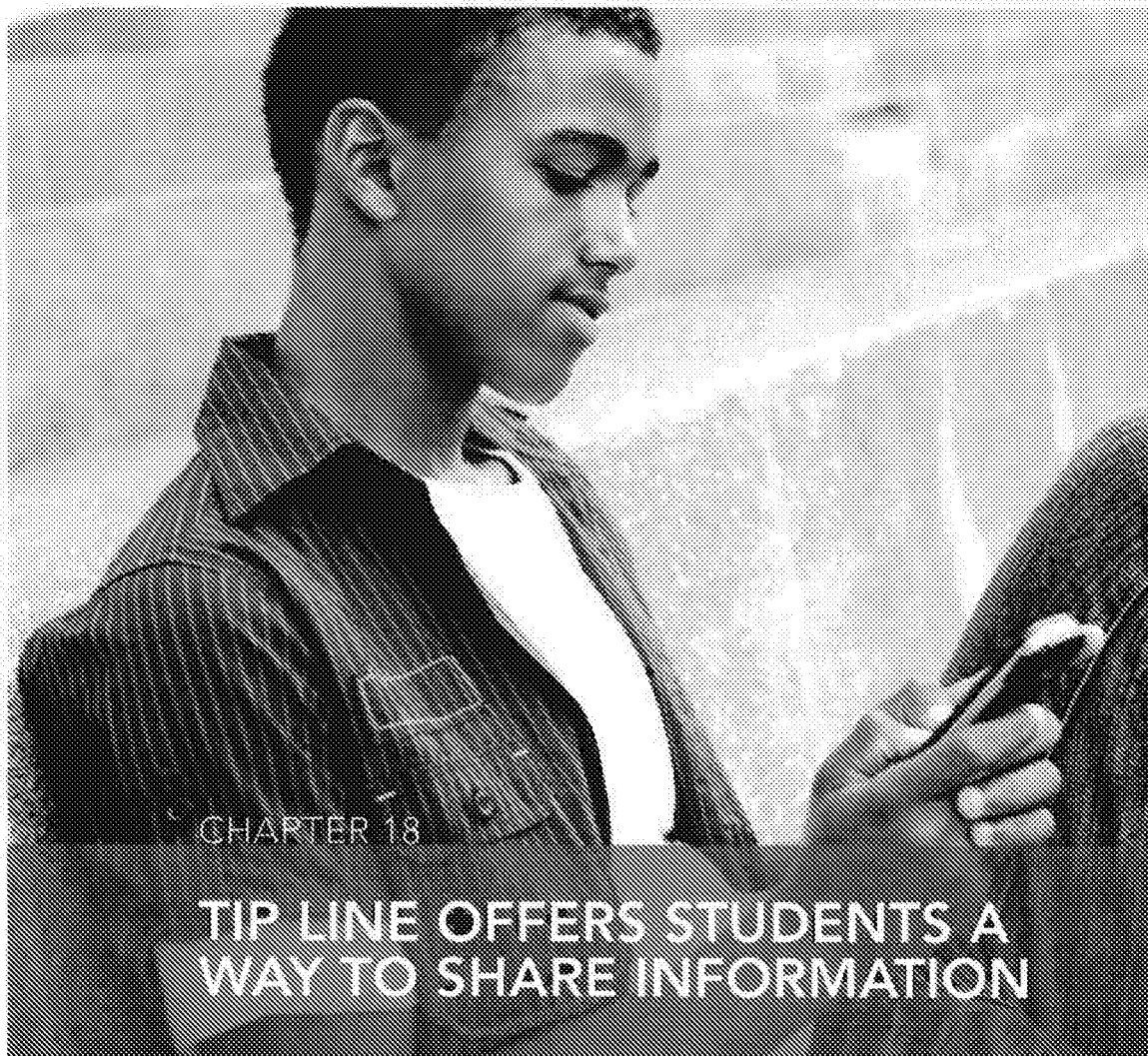
"There are skeptics when it comes to anonymous reporting and anonymous complaints. With this system, just because someone files a report, it doesn't trigger immediate action. It must go through a validation process and we must determine there is a valid need for an intervention. We don't just take everything at face value," he says.

*For more information on how these schools use their anonymous reporting software, contact Chief Gary Rudick, Tulsa Public Schools by email*

*at RudicGa@tulsaschools.org or by phone at (918) 746-6450; Garth MacDonald at Thomas Nelson Community College, email macdonaldg@tncc.edu or phone (757) 825-3450. A video on Tulsa's use of the software can be viewed at <http://www.youtube.com/watch?v=48kMkOZNa7o>*







## CHAPTER 18

# TIP LINE OFFERS STUDENTS A WAY TO SHARE INFORMATION

By Becky Lewis  
September 2013

Various schools  
Amherst, Ohio

*Should he tell someone what he's seen?*

*Can he make himself tell what he's seen?*

*Those thoughts chase themselves around in his head while he walks from class to class. Then he spots the gold and red and blue and black of a poster on the wall: Amherst Police Tip Line.*

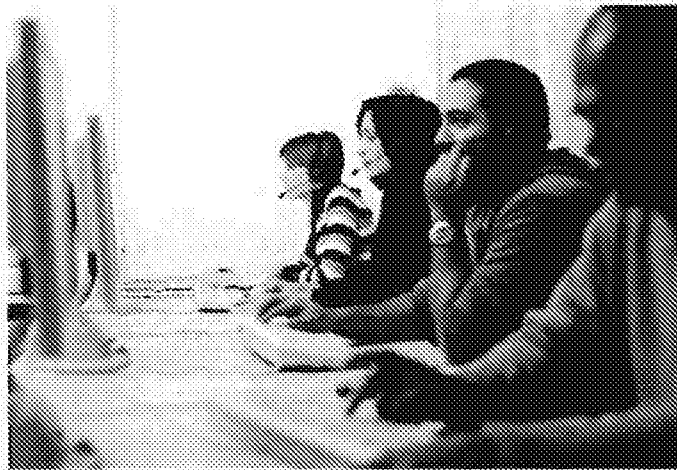
*He can tell. Without getting up the nerve to speak to someone he knows.*





Launched on Aug. 19, 2013, the day before classes began at Marion L. Steele High School, Amherst Junior High School and Walter G. Nord Middle School, the Amherst Police Tip Line accepts text messages from students and community residents, then converts them into written messages appearing on dispatch center computers. Dispatchers may be busy with emergency calls, but will read and respond to non-emergency tips and questions as soon as workload permits, usually within a few minutes.

Although not exclusively for use by the nearly 3,000 students enrolled at the three schools, the Amherst (Ohio) Police Department has promoted the Tip Line extensively in the town's three secondary schools, with a poster campaign and messages on the schools' Facebook pages. The posters encourage students to text the Tip Line if they have information on drug activity, alcohol activity, known underage drinking parties, planned fights, recent crimes, bullying, concealed weapons or concerns about others.



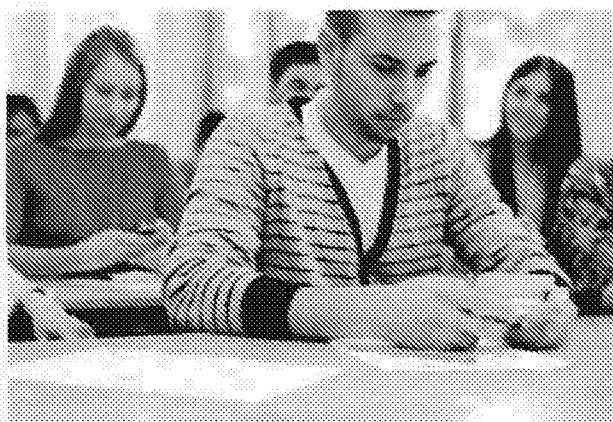
Police Chief Joseph Kucirek, a veteran of the detective bureau where he often reviewed cell phones as evidence, says "it just seems like kids and society in general text a lot of things they would never say. To give a juvenile, a student, the ability to text someone who can do something about a problem while the student remains in the background, can be a powerful thing. We want students to feel comfortable with telling us "Johnny's selling drugs, Bobby brought a knife to school."

And in the first few weeks of Tip Line use, Kucirek says his department already received one tip related to drug dealing that led to an arrest by a neighboring jurisdiction.

"We were looking at this way before Sandy Hook, and we worked on it through trial and error over the course of about two years," Kucirek says. "We knew we wanted a system where the dispatcher did not have to answer the phone to reply, because that could take them away from handling an emergency call. We looked at a lot of different options before we found one that let us do what we wanted."

What Amherst wanted to do was use a cellular phone line to receive the text messages, which the dispatchers could then answer using their terminal and keyboard rather than needing to answer the cellular phone and use it to respond to the text. If emergency calls prohibit an immediate response to pending text messages, the dispatchers get reminders every sixty seconds until text messages are answered.





"There are a lot of anonymous pay-for services out there where you have to text a five-digit number, which seemed very confusing. We also didn't want to have to deal with prank calls made by students who know they're anonymous. With this, just like when texting another cell phone, the numbers do show up. We can go back and find out who sent in the tip if we need to, but we would refrain from disclosing that information to other students," Kucirek says. "We did want to make it clear to the school, to the students, that pranksters or practical jokers could easily lose their cell phones as

evidence. But even with the number showing up, I still think the students will tell us things that they normally wouldn't."

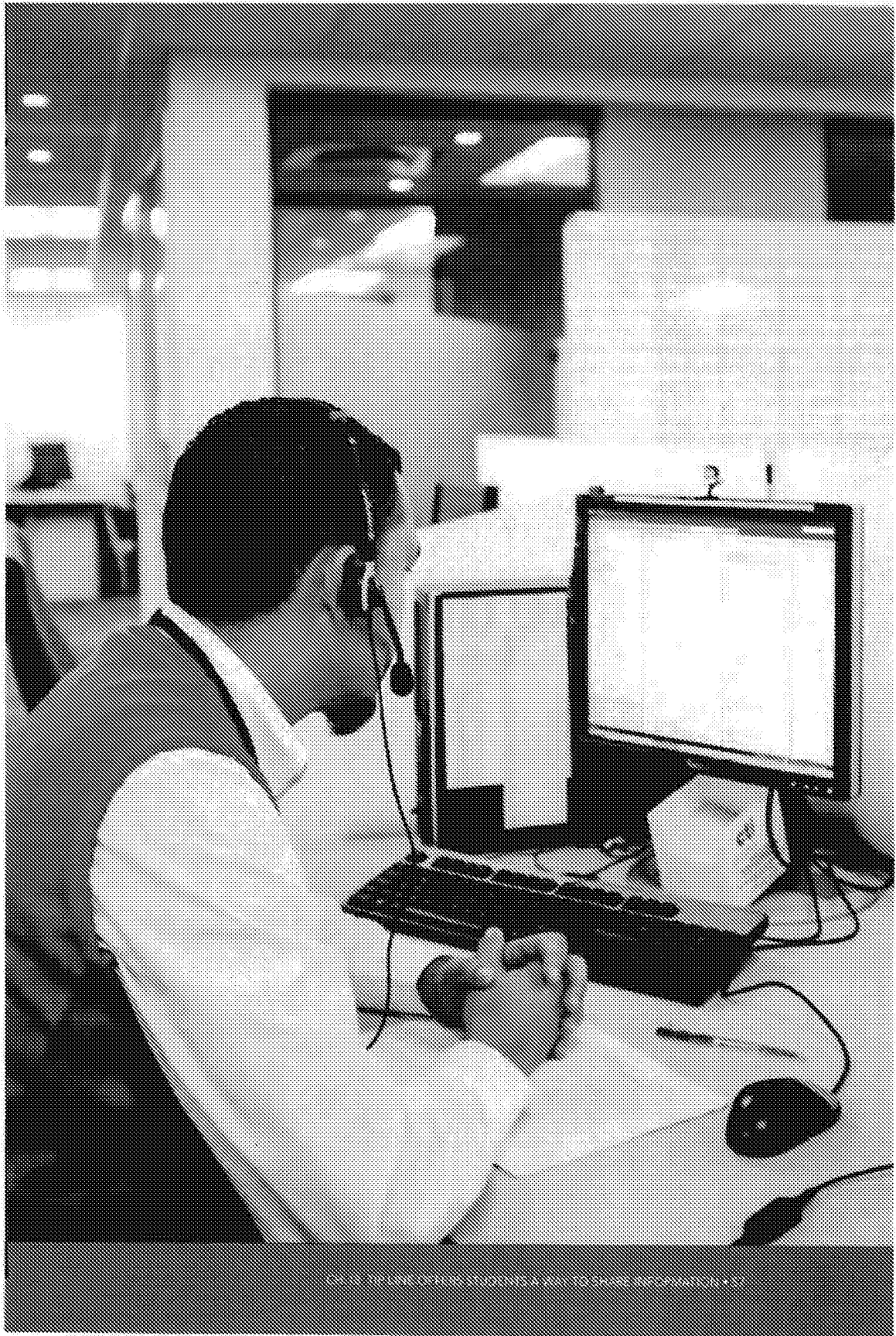
Kucirek says some of the 41 Amherst staff members helped with internal testing on the software for several months before the public launch, which included press releases on the department's website and Facebook page, Facebook publicity from the schools and elected officials, and extensive local media coverage.

"We launched it the day before school started to give students and their parents advance knowledge," Kucirek says. "Then, in addition to putting up the posters in the high school and junior high, we also spread the word to the elementary school staff, because they have cell phones even though most of the children don't."

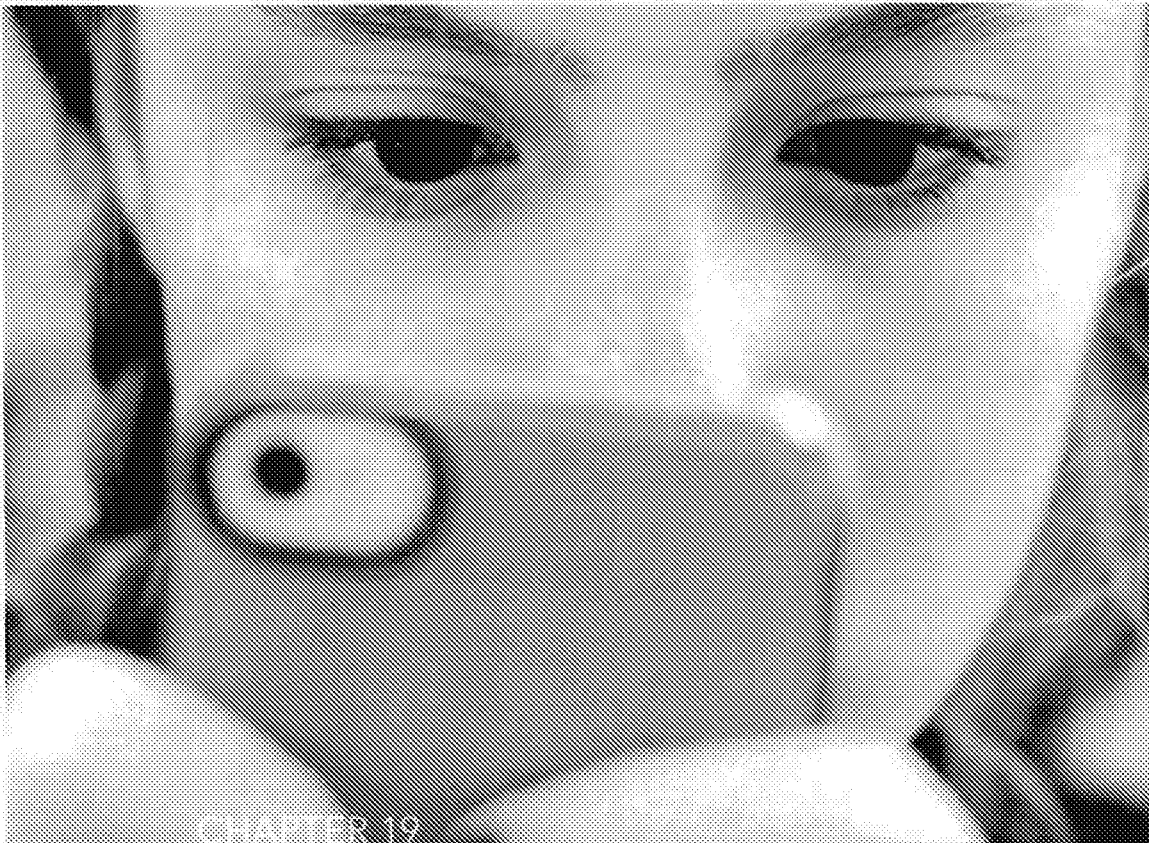
Although the Amherst Police Tip Line generally should not be used in emergency situations, it could be used by hearing/speech impaired persons or by someone who is in a situation where talking could present a danger. Adults as well as students can use it provide tips, and the Tip Line can also be used to ask non-emergency questions such as "What night is trick or treat night?" Also, in this town of about 13,000 residents located some 30 miles from Cleveland, dispatch handles after-hours calls about problems with utilities, which can tie up phone lines. Residents sending a text message about an outage instead of calling could help alleviate that problem, Kucirek says.

For more information on the Amherst Tip Line project, visit <https://www.facebook.com/AmherstPoliceDepartment>, <http://www.amherstpolice.net/> or email [amherstpolice@amherstpolice.net](mailto:amherstpolice@amherstpolice.net).









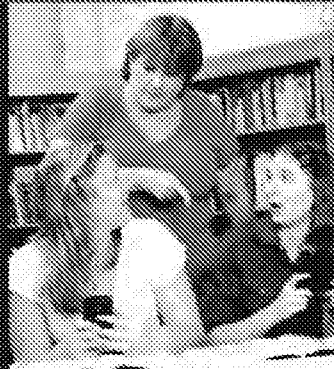
## CHAPTER 19

# "SEE-HEAR-REPORT" REACHES OUT TO SOMERSET STUDENTS

By Becky Lewis  
February 2013

**Various schools  
Somerset, Ky.**

*Like many other law enforcement agencies around the country, the one in Somerset, Ky., periodically holds training for active shooter scenarios, with administrators hoping at the same time the training never needs to be put to use.*





*In late January 2013, the department took a step aimed at preventing that type of situation with the introduction of "See-Hear-Report," an anonymous text-a-tip program aimed at students in the county's 20-plus rural and small town schools.*

"Our department has been very progressive over the years in a number of different programs. Our acting chief, Doug Nelson, saw a Colorado program that targeted bullying via an anonymous text-a-tip program, and he wanted to start the same type of program here because students and young adults are so very comfortable with sending text messages," says Lt. Shannon Smith.

After exploring several possible options, the Somerset Police Department settled on a service used by a number of agencies across the nation, and targeted efforts toward students in the county's three high schools.

Smith says the service provides students with an assurance of anonymity and confidentiality, but at the same time allows the department to track the information through its system to ensure that all tips receive appropriate followup.



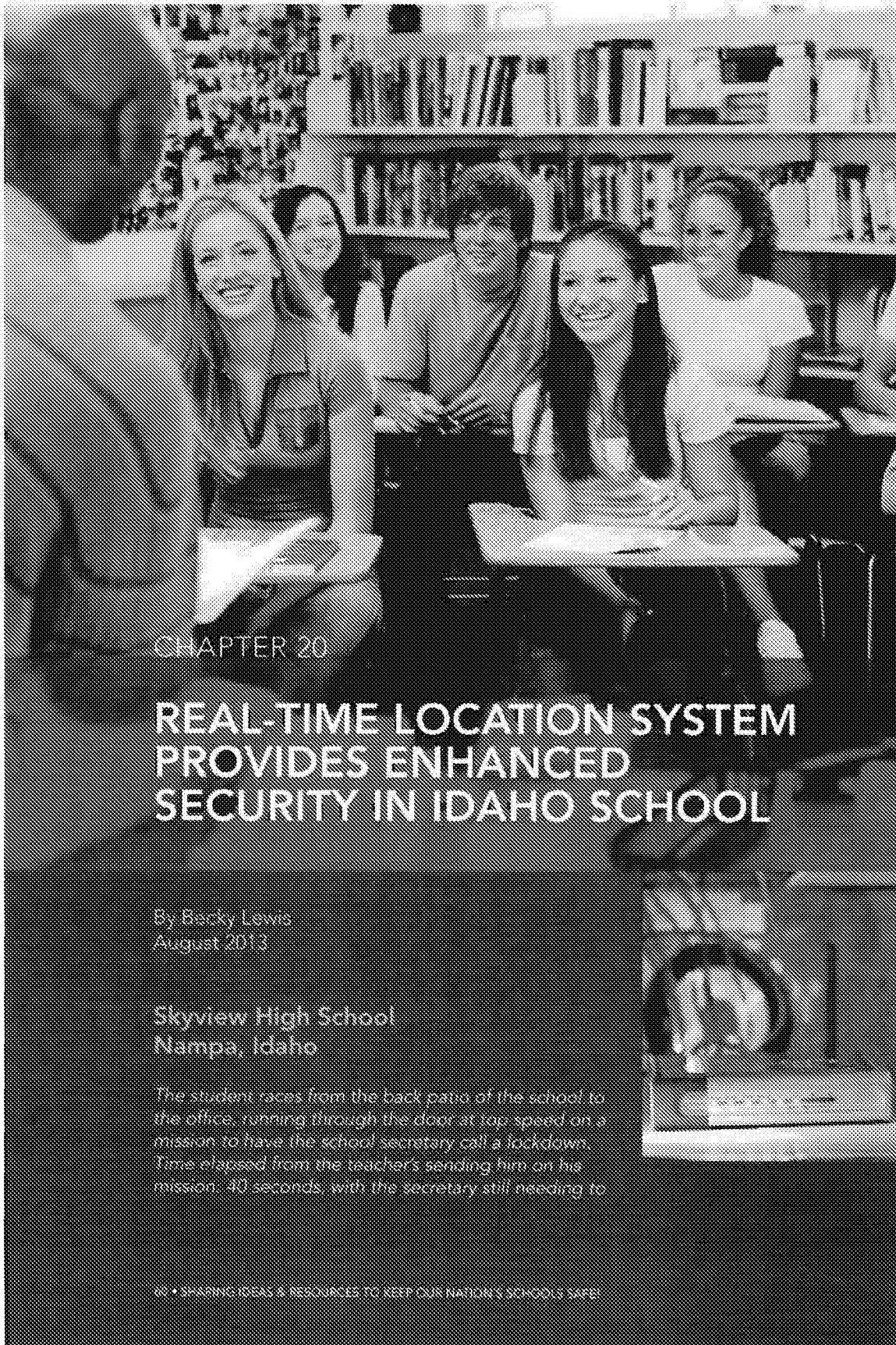
"Reports indicate that in a number of the situations involving active shooters in schools in this country, other students knew about it beforehand and didn't tell anyone, maybe because they were fearful, or embarrassed, or didn't think it was their place to tell," Smith says. "With See-Hear-Report, they will be guaranteed confidentiality without fear of retaliation. We do a lot of things in our department geared toward response and handling these types of situations, such as for a number of years we've sent our officers to active shooter training and conducted in-house training on active shooter response. We want to market this toward the prevention end of things and give the students an opportunity to stop an event before it takes place."

The 40-officer department also plans to keep up with the active shooter training, including a refresher course that took place over the December 2012 holiday break at one of the local high schools in Somerset itself (population 11,300; the county's population is 60,000).

"It was pretty well set up when news of Sandy Hook came down," Smith says. "It hit us hard like anything does that has to do with kids being injured or killed, but there was a sense of satisfaction that we were not in the same situation as many other departments watching this on the news, because most of them were not just days away from sending the entire department through a refresher course in a actual school building. We always try to be progressive and we've trained and prepared in the event anything ever takes place, but we also want to do whatever we can to prevent something from happening."

For more information, visit <https://www.facebook.com/SomersetPolice>.





## CHAPTER 20

# REAL-TIME LOCATION SYSTEM PROVIDES ENHANCED SECURITY IN IDAHO SCHOOL

By Becky Lewis  
August 2013

**Skyview High School  
Nampa, Idaho**

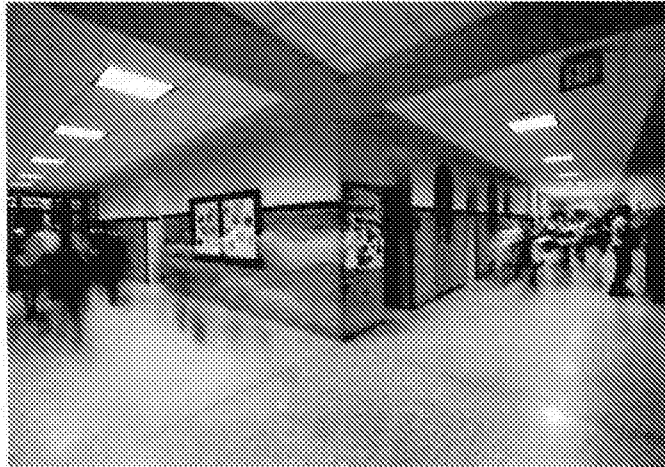
*The student races from the back patio of the school to the office, running through the door at top speed on a mission to have the school secretary call a lockdown. Time elapsed from the teacher's sending him on his mission: 40 seconds, with the secretary still needing to*



*call the lockdown on the PA system, make sure the school resource officer receives the alert and call 911. Actions that would have taken even more precious seconds had this not been a drill.*

*A teacher pulls down on the emergency tab on her alert tag, automatically putting the school on lockdown, bringing the SRO on the run and alerting 911 dispatch to send more officers to the SRO's location. Time elapsed until the SRO arrives in her classroom: 3.9 seconds.*

Skyview High School in Nampa, Idaho, became the first school in the United States to implement use of a real-time location system (RTLS) that uses radio frequency identification (RFID) technology and the school's existing Wi-Fi network in April 2013. Installation of the system came as the result of concerns felt by Officer Brad Ford, Skyview's SRO, after the Sandy Hook Elementary shooting in December 2012.



"We protect our banks and our houses better than we do our children, and our children are the most valuable resource we have. It's my job to ensure that when parents drop their kids off, I'm providing the best security I can, and I believe with this system, that's what we're doing," Ford says.

Ford says in the course of his research into automated ways to call a lockdown, he considered pull-station alarms, "panic buttons" on walls and various types of computer software, but ultimately recommended this system to the administration at Skyview High and his superiors at the Nampa Police Department because the wearable device travels with the school's 100 teachers and staff wherever they go: classrooms, the gym, the cafeteria, the outside patio. The vendor had previously marketed this system to medical facilities such as hospitals, nursing homes and mental health centers, but proved readily receptive to adapting it for use in a school. A pull on the emergency tab activates lockdown procedures and sends device location information to the school's computer network, the SRO and the 911 dispatch center. The device also includes two programmable buttons that summon lesser tiers of help in the event of a medical situation or a student who is disruptive, but not perceived as a threat to the entire school. Although the school has not needed to use the system to call a lockdown – and both Ford and Nampa Police Chief Craig Kingsbury hope a lockdown never happens – several calls using the two buttons have already proved the system's worth.





"We all have to deal with medical issues and unruly students too, and that's how the device has already proven beneficial to us," Ford says. "We didn't want a device that just does one thing, we wanted one that can do multiple things. We selected this system, the vendor brought in two people to map out the school and the next day all the staff had tags."

An anonymous funding donation from the community also contributed to the speed with which Skyview implemented the system. Kingsbury said the

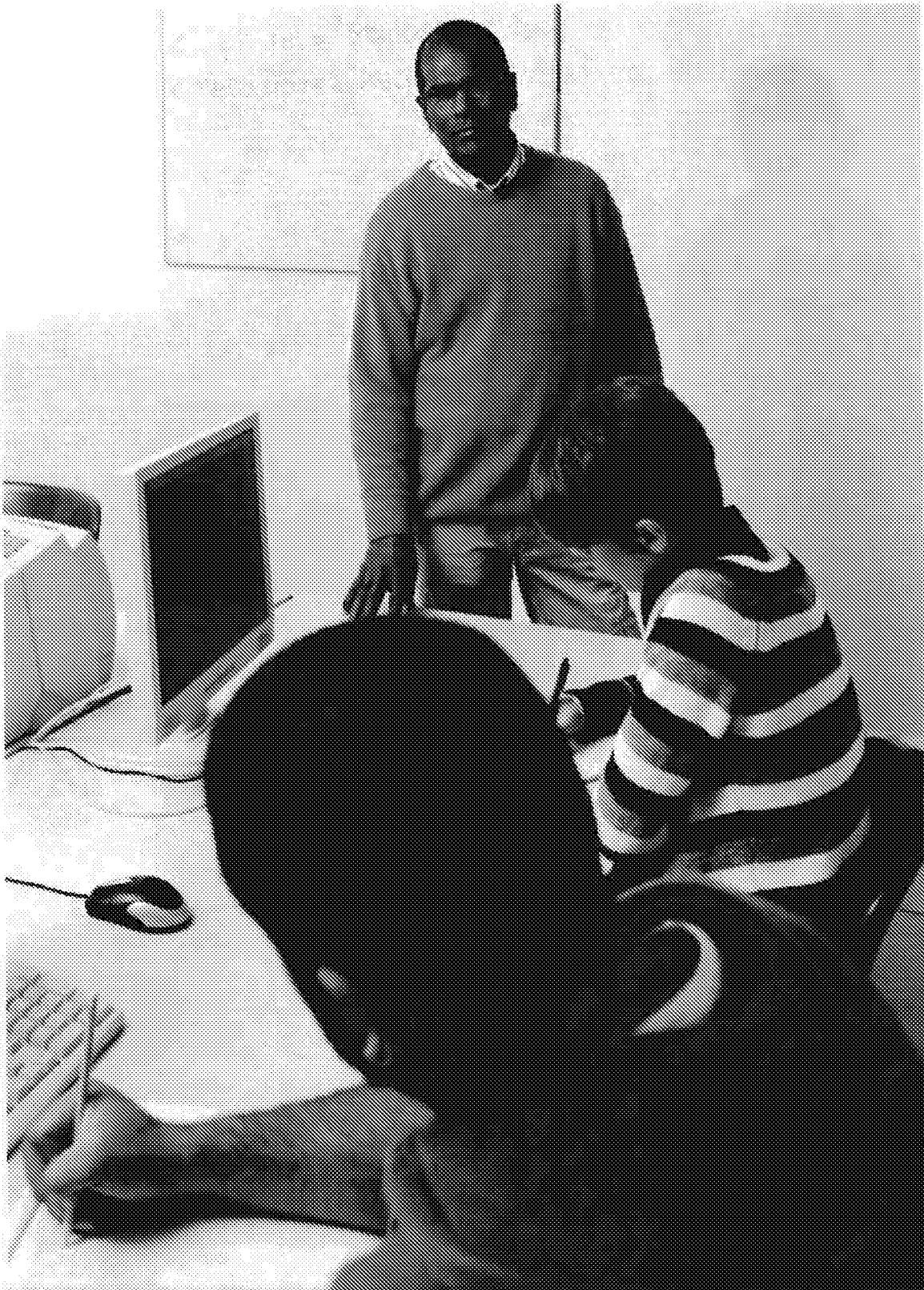
quick installation would not have happened without that donation: "It's not an inexpensive system, but it works very well. The school staff is very receptive. The other schools in the area want to know when they can get it. It is something that gives our school staff, our parents and our community a sense of security."

The other schools in Nampa (population 80,000-plus) include 12 public elementary schools, three middle schools and three high schools, plus a number of private schools, all falling under the jurisdiction of a police department with 112 full-time sworn officers and more than 100 other staff and volunteers. It will take more than donations to fund expansion of the system, but Kingsbury says there have been discussions with the Governor's Task Force on School Safety and with state legislators about funding sources, and the system has been demonstrated for the Idaho Chiefs of Police, the Idaho Sheriffs Association and other school districts.

"Top-level administrators across the state have seen demonstrations and everyone who has seen it is excited about it. Cost is always a concern, of course, as is making adjustments to meet the needs of schools in rural areas," Kingsbury says. "I want to emphasize this is not a catch-all. It's a way to deal with quick lockdown/rapid response situations. Schools and law enforcement still need to be cognizant about the physical structure and know which doors are locked, the procedures for entry and so on. This is just a component of a school safety plan, one to use if there is a catastrophic event. You can't forget the need to maintain and prevent."

*For more information on Skyview High School's use of real-time location system technology, contact Officer Brad Ford at (208) 340-0603 or by email at [fordb@cityofnampa.us](mailto:fordb@cityofnampa.us).*









## CHAPTER 21

# PROVIDING A DIRECT CONNECTION BETWEEN SCHOOLS AND LAW ENFORCEMENT

By Becky Lewis  
June 2013

### Sweetwater Independent School District Sweetwater, Texas

When the boy wouldn't return to his seat, when he began walking toward the front of the classroom, aggression showing in every nuance of his body language, the teacher knew she needed help. She also knew that verbalizing that call for help might provoke the enraged teen even further, so, while still trying to talk to him in a calm voice, she casually walked behind her computer and past it again, reaching out to flick the mouse over an icon on the desktop. Seconds later, help was on the way.

68 • SHARING IDEAS & RESOURCES TO KEEP OUR NATION'S SCHOOLS SAFE





A new emergency alert software released in spring 2013 allows teachers and other school staff to instantaneously, silently send emergency alerts directly to local law enforcement officers in their patrol cars, the local dispatch office and to the registered cell phones of other teachers and administrators in the same school building and to the computers in all the other classrooms. The town of Sweetwater, Texas (population approximately 12,000), and the local sheriff's office became the first municipality and county in the nation to go live with the service on May 1, following a month of setup and training.

"I hope and I pray every day that we won't ever need it, but we're ready if we do," says Sweetwater Police Chief Brian Frieda. "Once the school district heard about it, they pounced on it. There's no sense in hesitating to use some good technology that helps with security of our kids."

The emergency alert creates a chat room among the computer sending the alert, the responding officers and the local dispatch center, which permits them to communicate information about the emergency in real-time. Responding officers can also click a link and view a diagram of the school and a map showing the school's location.

Frieda and the Sweetwater Police Department heard about the software from Nolan County Sheriff David Warren, who played an instrumental role in helping introduce the concept to the Sweetwater Independent School District. The district serves approximately 2,300 students from pre-kindergarten through 12 on six campuses: one high school, one middle school, three schools each housing two elementary grades and a pre-K center. The police department and the school system have already held several drills with the software, and Frieda says his department will incorporate it into its active shooter training this summer, when his 22 sworn officers and two reserve officers will use one of the school buildings for scenario training.

"Once the school year starts, we will have a series of scenario drills where teachers launch the system and get comfortable with it. We've already heard from other nearby school districts that they're interested in implementing it as well," Frieda says. Drills will involve both the use of the silent alarm and the chat room function, wherein the teacher, or a student designated by the teacher, uses the computer to send instant messages with additional information to school personnel, responding patrol vehicles and dispatch.

Frieda explains that if the initial activation isn't aborted within seconds, officers immediately respond in a manner similar to the way they would to a 911 hang-up call. Receiving an alert, even with no further information, provides the agency with the exact location of the alarm and gives officers access to a diagram of the campus and GPS directions to the location: "This gives us more of a tactical advantage. As officers arrive on the scene, they can take a quick look and increase their situational awareness."

"I have it set up to come across my desktop at work, the laptop in my car and on my smartphone. That lets me keep up with everything that's going to the officers," he adds.

For more information, contact Sweetwater Police Chief Brian Frieda at [bfrieda@cityofsweetwatertx.com](mailto:bfrieda@cityofsweetwatertx.com).





## CHAPTER 22

# REAL-TIME COMMUNICATIONS COMES TO OREGON SCHOOL

By Becky Lewis  
July 2013

**Shady Cove Middle School  
Jackson County, Ore.**

The alert comes into the sheriff's office command center. Someone pushed the alarm button in Classroom 10. All over the school, doors automatically close and the building goes into immediate lockdown. Live video feed comes into the command center, and an officer starts two-way communication with the teacher who hit the button. The teacher who heard gunshots echoing from down the hall.





Thanks to the efforts of the Jackson County Sheriff's Office, Shady Cove Middle School in Jackson County, Ore., became the first school in the nation to use a new technology that provides a real-time direct link between law enforcement, first responders and the school in the event of an emergency – be it medical, fire or criminal in nature. The sheriff's office used drug seizure money to purchase the system, and local businesses Precision Electric and Adroit Construction donated installation labor over the Memorial Day Weekend.

When a teacher (or a student in the event the teacher is incapacitated) pushes the alarm button, cameras located in the classroom and elsewhere in the building begin providing live-time video feed to the sheriff's office command center and to school administrative offices. According to Sheriff Mike Winters, the ability to see what is going on inside the building in real-time could prove invaluable in the amount of time – and potentially lives – saved in the event of an emergency. That's why when he was offered the opportunity to pilot the system, he was quick to move on the project, selecting Shady Cove because "I wanted a school that had great teachers with an absolutely 'can do' attitude. The administrators of School District 9 are the same way. They really care about their students' safety. They were really amazed at what the technology could do and they wanted to be part of it."



With the system in place, the sheriff's office and the school district worked together to run drills and come up with policies and procedures before Jackson County (population 206,000, some 75,000-plus in the county seat, Medford) formalizes plans to implement the system in additional schools.

"I've never seen a better system for implementing real-time communication. It really gets the job done," Winters says. "The beauty of this system is when the alarm is pushed and the cameras come up, we're looking at real-time info and we can brief officers. From the sheriff's office in Medford, we can open doors and change the status lights. We can visually search the school while the first responders are in route and if there is a shooter in a classroom, we can put that light to red and the others on green to direct the first arriving officers to the crisis spot. With the pending addition of an app for officers' smartphones, they will be able to look at the same information as well as receiving direction from headquarters. "

And if the doors go into lockdown with the shooter outside the classrooms, he might spend time going from door to door, looking for entry, while officers get closer. "Time saved equals lives saved. Activating this system might not save everyone in a shooting incident, but it might substantially reduce the number of



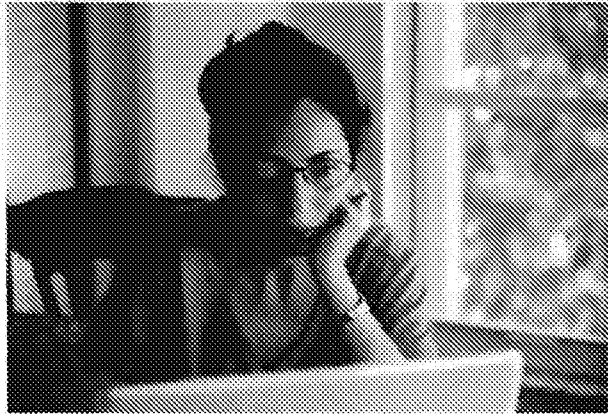


ALL SHARING IDEAS & RESOURCES TO KEEP OUR NATION'S SCHOOLS SAFE!



fatalities. We might even be able to use the two-way communication channel to engage the shooter and distract him with the information that police are nearly there."

And while Winters, like every other law enforcement officer in the country, hopes that Jackson County never needs to use the system during a school shooting, he's glad it's in place, and he notes it could also be used to call for medical help or report a fire and improve outcomes in those types of situations: "If fire services could see immediately that one wing of a school is fully involved, they'd know to go to more alarms immediately. EMS could go into situations better prepared. This is asset management at its best."



*To learn more about the system and its implementation at Shady Cove Middle School, contact Public Information Officer Andrea Carlson at (541) 864-8801, email [carlsoak@jacksoncounty.org](mailto:carlsoak@jacksoncounty.org). To watch a video about the implementation of the technology, visit [http://www.youtube.com/watch?feature=player\\_embedded&v=XapKQsbX5u8](http://www.youtube.com/watch?feature=player_embedded&v=XapKQsbX5u8).*





## MUNICIPAL WORKERS WATCH OVER NEIGHBORHOOD STREETS

By Becky Lewis  
May 2013

### My Community on Patrol New Jersey

*There's a lockdown situation at the local high school. Police, firefighters and EMS personnel know where to go, what to do. As do the sanitation workers in the vicinity of the campus.*

*Most communities are well aware of the roles that public safety professionals can play in such an event, but sanitation workers? Well, if they participate in a New*



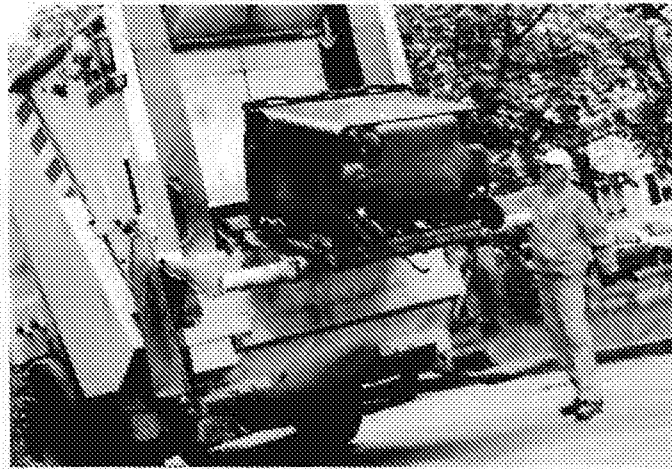
70 • SHARPING IDEAS & RESOURCES TO KEEP OUR NATION'S SCHOOLS SAFE!



*Jersey project called My Community on Patrol (M.C.O.P.), those workers know their trucks can make excellent roadblocks that can help keep the public away from the danger and free up law enforcement officers from routine traffic control duties.*

Freeholder\* James Polos, chair of the Middlesex County Department of Public Safety and Health, introduced the Middlesex Community on Patrol program in 2003 as a way of using county employees as "extra eyes and ears" in the community to help local law enforcement. The successful program expanded statewide in 2007 and changed its name to one that reflected that expansion, but retained the M.C.O.P. acronym and branding.

"The idea behind it is simple: in many communities, particularly small ones, there's a limit to the number of police personnel patrolling the streets. At any given time during the day or even during the evening, there can be significantly more municipal employees on the streets than there are police officers," Polos says. "I'm talking about sanitation workers, housing inspectors, fire inspectors, bus drivers, senior citizens transport drivers.



They're all out on the street, day in and day out. They have a keen knowledge of what the community is about. If they travel the same route regularly, they may have a keen awareness of what looks out of place, such as a suspicious vehicle in driveway or a garage door that's open when it shouldn't be."

Participation in M.C.O.P. is voluntary; employees who choose to become involved take a two-hour training program about what to watch for and how to report it, using the two-way radio and frequencies already in use in their vehicles. The Middlesex County Prosecutors Office and the Middlesex County Chiefs of Police Association helped develop the training, which has reached approximately 2,000 employees in Middlesex County alone in the past 10 years.

"We've really instructed them to become more keenly aware of their surroundings. If they think something doesn't seem right or look right, they should report it," Polos says.

And implementing M.C.O.P. has given rise to a more holistic response to a potential incident in a school: "Across the country, there's been an enormous amount of focus on the public safety response to situations in schools, but not much emphasis on the community response. As an example, we looked at other resources we could use in establishing inner and outer perimeters that don't tax the limited emergency personnel available and decided there's no better barrier than a trash truck!"





Polos says M.C.O.P. has created a “small army of volunteers” in communities throughout New Jersey. Middlesex County participants who call in reports receive recognition, which helps maintain worker interest in continuing with the program.

“The resources they can provide are limitless. If we’re looking for someone involved in a school violence incident, for a missing child, for a hit-and-run driver, it puts more eyes on the street. We’ve recently expanded the program so that in certain instances, they may receive a communication through

their radios to be on the lookout, for example, for a particular individual or car,” he says.

“We do stress that they are not to pursue anyone or try to apprehend anyone. They’re simply acting as eyes and ears,” Polos adds.

*If you’re interested in establishing a program in your community based on M.C.O.P., please contact James Polos at [freeholder@mpm-nj.com](mailto:freeholder@mpm-nj.com).*

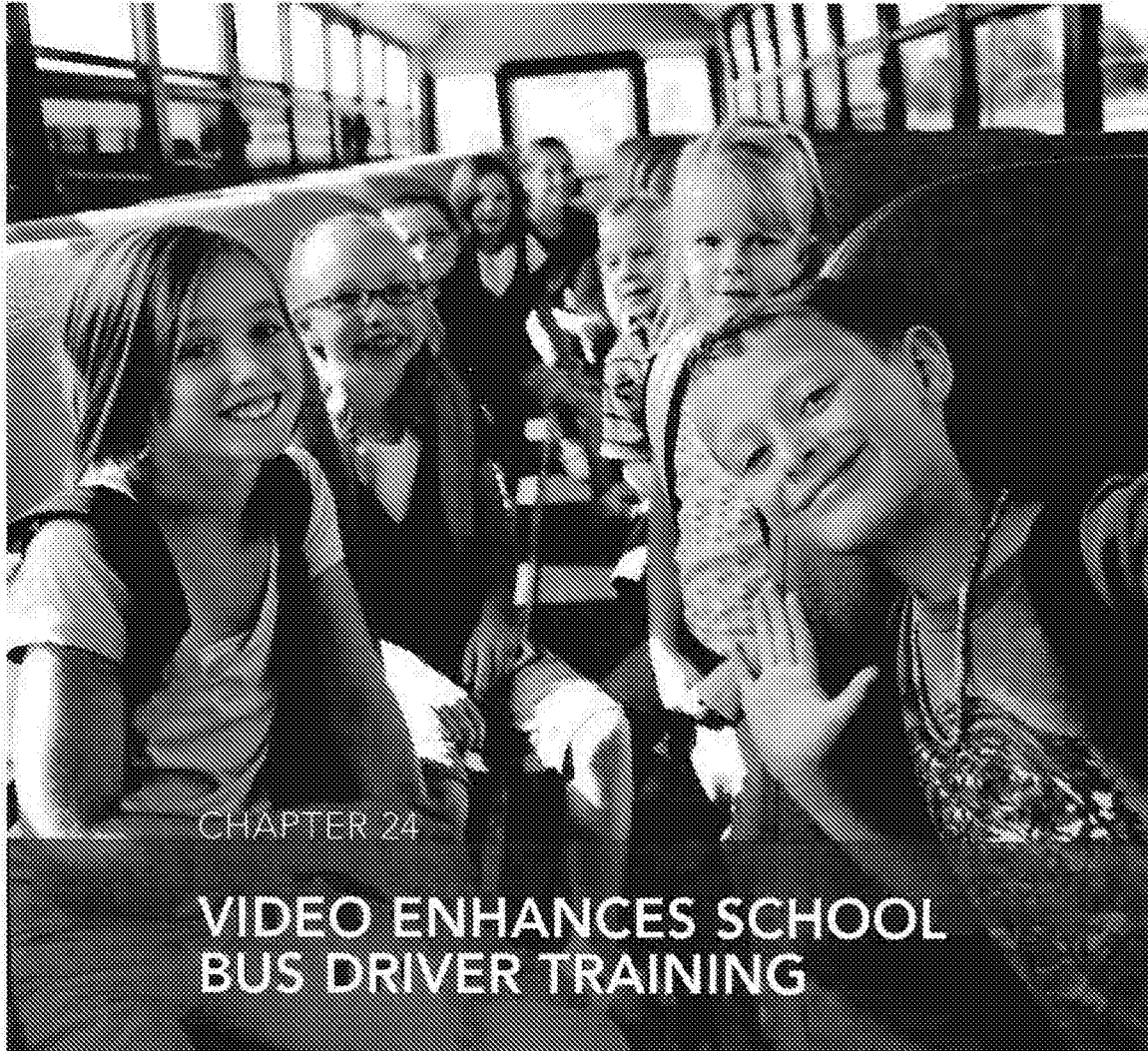
\*The Board of Chosen Freeholders is the county legislature for New Jersey counties.





CH-23: MUNICIPAL WORKERS WATCH OVER NEIGHBORHOOD STREETS • 71





## CHAPTER 24

# VIDEO ENHANCES SCHOOL BUS DRIVER TRAINING

By Michele Coppola  
May 2013

### Anne Arundel County Public Schools Maryland

*Glancing in her rearview mirror, the bus driver doesn't see any kids who are acting up. What she does see is an older student standing right behind her with a gun in his hand.*

Victoria Williams, safety and training manager for the Transportation Division of the Anne Arundel County (Md.) Public Schools, says the division uses a 25-minute video simulating the hijacking of a school bus to augment its preparedness, safety and awareness training for bus drivers, bus attendants and cab





drivers. Cab drivers sometimes transport students with special needs to schools inside and outside Anne Arundel County. Bus attendants ride on buses transporting special needs students.

To date, the division has trained approximately 1,059 drivers and attendants using the School Transportation Security Awareness DVD, produced several years ago through the U.S. Department of Homeland Security Transportation Security Administration. The division holds refresher training sessions periodically.

The Anne Arundel training program incorporates discussion on safety and security awareness, including the purpose behind pre-trip bus inspections and the importance of driver awareness of any activity that may be suspicious.

The video depicts the hijacking of a school bus that ends with the safe release of the students. It emphasizes preparedness, teamwork, actions by the bus mechanic and the bus driver, and good communication throughout the event based on a security plan.

Williams says drivers appreciate the video as part of their training and she would recommend it to other school districts.

"Their eyes are really opened up by it, and there are always a lot of follow-up questions,"

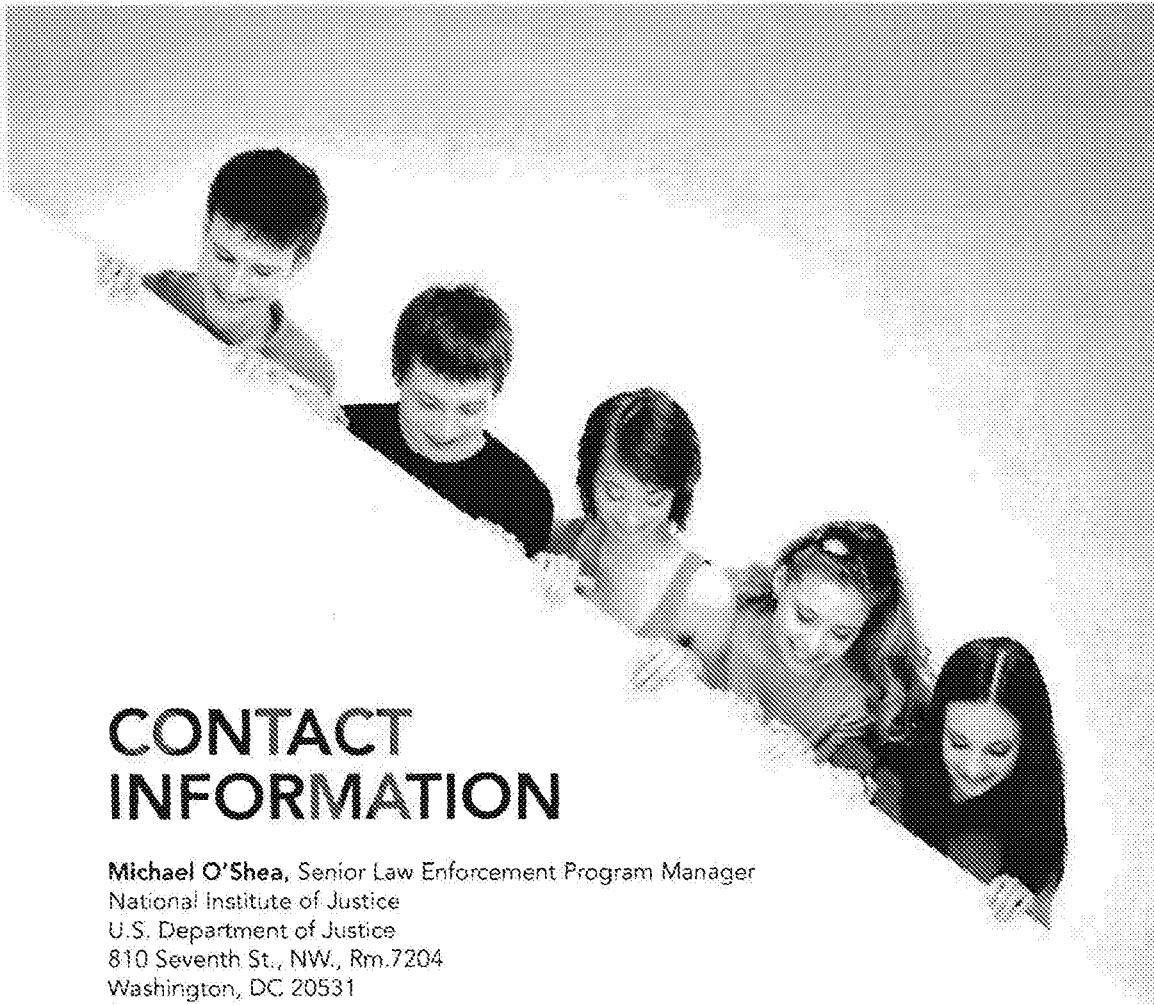
Williams says. "It's a teamwork situation between the mechanics, the schools and the bus drivers. Communication is extremely important. When we showed it the very first time, the drivers were sitting on the edge of their seats. You could hear a pin drop. It totally had their attention 100 percent."

"The drivers are our eyes and ears," she adds. "When they see something of a suspicious nature, suspicious activity of any kind, they should call it in. We are out there every day and we know our neighborhoods, we know our roads. We even had a bus driver call in because a car was following the bus. It turned out to be one of our area specialists, but it was a good thing to do. Drivers need to use common sense and good judgment."

For more information on the Anne Arundel County program, contact Victoria Williams at [vlwilliams@aacps.org](mailto:vlwilliams@aacps.org). To view the TSA video, visit <http://www.tsa.gov/stakeholders/school-transportation-security-awareness>.







## CONTACT INFORMATION

**Michael O'Shea**, Senior Law Enforcement Program Manager  
National Institute of Justice  
U.S. Department of Justice  
810 Seventh St., NW, Rm.7204  
Washington, DC 20531  
(202) 305-7954  
michael.oshea@usdoj.gov

**Lance Miller**, Director  
National Law Enforcement and Corrections Technology Center-National  
700 N. Frederick Ave.  
Bldg. 181, Rm. 1L30  
Gaithersburg, MD 20879  
(800) 248-2742  
(301) 240-6731  
lmiller@justnet.org

Visit <http://www.schoolsafetyinfo.org> for access to up-to-date publication and website resources. New success stories similar to the ones in this publication are added on an ongoing basis. To suggest a success story topic, contact Senior Writer Becky Lewis at [rebecca.l.lewis@lmco.com](mailto:rebecca.l.lewis@lmco.com)

Free school safety resources can be downloaded from <http://srtbrc.org/2012/12/free-school-safety-resources/>, the website of the NLECTC System's Small, Rural, Tribal and Border Regional Center.





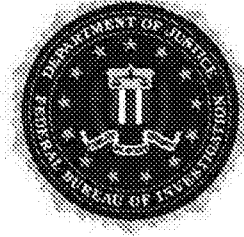
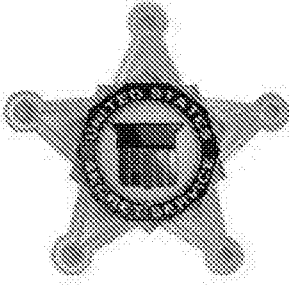


Knowledge & Partnership  
Save Lives

**NIJ**







# Press Release

April 15, 2010  
Contact: 202-406-5708  
GPA 03-10

## **NEW STUDY OF TARGETED VIOLENCE AFFECTING U.S. INSTITUTIONS OF HIGHER EDUCATION RELEASED**

***U.S. Secret Service, U.S. Department of Education and Federal Bureau of Investigation  
Collaborate on Joint Effort***

WASHINGTON, D.C. – On Friday, April 16, 2010, the U.S. Secret Service, the U.S. Department of Education and the Federal Bureau of Investigation will release a study of targeted violence incidents on U.S. campuses of higher learning.

The June 2007 *Report to the President on Issues Raised by the Virginia Tech Tragedy* included a recommendation that the Secret Service, Department of Education and the Federal Bureau of Investigation explore the issue of violence at institutions of higher education. This collaborative effort examines the scope of the problem of targeted violence at U.S. institutions.

In total, 272 incidents were identified through a comprehensive search of more than 115,000 results in open-source reporting from 1900 to 2008. The incidents studied include various forms of targeted violence, ranging from domestic violence to mass murder. The findings should be useful for campus safety professionals charged with identifying, assessing and managing violent risk at institutions of higher education.

The study and its findings will be available on each of the agencies' Internet sites:  
[www.secretservice.gov](http://www.secretservice.gov), [www.ed.gov](http://www.ed.gov) and [www.fbi.gov](http://www.fbi.gov).

###

*EDITOR'S NOTE - For questions concerning the study or its findings, contact the U.S. Secret Service Office of Government and Public Affairs at 202-406-5708, the Department of Education Office of Public Affairs at 202-401-1576 or the FBI Office of Public Affairs at 202-324-3691.*



[REDACTED] RMD)(CON)

b6  
b7C

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Tuesday, September 10, 2013 1:21 PM  
**To:** [REDACTED]  
**Subject:** FW: Campus Active Shooter Conferences and Tabletop Exercises --- UNCLASSIFIED

b7E

Classification: UNCLASSIFIED

=====  
TRANSITORY RECORD

CLAs --

FYSA

The email below went to all Active Shooter contacts in the field. The email group includes numerous ASACs.

An email should soon be going to all SACs on the same subject, requesting their support.

[REDACTED]  
SS [REDACTED]  
Program Manager  
Campus Liaison Initiative

b6  
b7C

[REDACTED]  
Counterterrorism Division - FBIHQ  
[REDACTED]

**From:** [REDACTED] (DO) (FBI)  
**Sent:** Tuesday, September 10, 2013 11:22 AM  
**To:** [REDACTED]  
**Subject:** Campus Active Shooter Conferences and Tabletop Exercises --- UNCLASSIFIED

b7E

Classification: UNCLASSIFIED

=====  
TRANSITORY RECORD

Good afternoon,

Thank you for your continued effort to host Active Shooter conferences and tabletop exercises with your state and local law enforcement. I wanted to advise you that I will take over as primary POC for emails of concern regarding the program.

As we continue to expand the Active Shooter initiative, we would also like to emphasize the importance in reaching our campus public safety partners. We continue to receive strong Field EM support for this effort and would ask that you also include conferences and TTXs for campus public safety in your AOR. On the SIOC Active Shooter site, you can find the campus specific TTX, which would be scheduled for the last part of the second day of the campus active shooter conference.



Your field office Campus Liaison Agent (CLA) can coordinate the campus TTX and invite the appropriate campus public safety leaders. The roster of CLAs can be found on the Campus Liaison Initiative (CLI) website

[redacted]

b7E

An EC describing this responsibility was uploaded to all CLAs last week from the FBIHQ Campus Liaison Initiative. Please see [redacted] I invite you to share this with your EM, ASACs, CMC and Training Coordinators, as appropriate.

Please let us know if you have any questions and thank you for your continued support of the active shooter program.

[redacted]

b6  
b7C

[redacted]

Special Advisor

Tel [redacted]

BB [redacted]

[redacted]

b6  
b7C

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



## Lead Information

Type: Action Required  
Precedence: Routine

Created: 08/30/2013  
Due: 10/29/2013

From: COUNTERTERRORISM, DG-OPS2 [REDACTED]

Contact: [REDACTED]

Phone: [REDACTED]

Drafted By: [REDACTED]  
Approved By: [REDACTED]

UC [REDACTED]  
A/ASC [REDACTED]  
A/SC [REDACTED]

Case: [REDACTED]

Lead: 3

Reference Document: [REDACTED]

Details: (U) Field Offices will invite campus public safety commanders to Active Shooter Command Staff Seminars and schedule Active Shooter Tabletop Exercises using the specific scenario developed for institutes of higher education on CIRG's Active Shooter website. Campus public safety departments, if armed and sworn, will also be offered tactical ALERRT training.

Location 1

To: ALL [REDACTED] COORDINATORS  
Attn: Campus Liaison Agent

Status: Covered

Recipient: ALL [REDACTED] SUPERVISORS

Coverage Action: Lead fully covered on 09/04/2013 by [REDACTED]

Comments: (U) [REDACTED] covered as per [REDACTED] SSA [REDACTED]

Activity Log

b6  
b7C  
b7E

b7E

b6  
b7C  
b7E



[REDACTED] (RMD)(CON)

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Friday, September 06, 2013 9:27 AM  
**To:** [REDACTED]  
**Cc:** [REDACTED] (DO) (FBI)  
**Subject:** FW: Active Shooter Initiative 8.28.2013 --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

FYSA

**From:** [REDACTED] (DM) (FBI)  
**Sent:** Wednesday, August 28, 2013 9:54 AM  
**To:** [REDACTED] (DM) (FBI)  
**Subject:** Active Shooter Initiative 8.28.2013 --- UNCLASSIFIED

b6  
b7C

Classification: UNCLASSIFIED  
=====

Greetings AS POCs - Just three quick things:

- A reminder that **members of the media are not allowed to attend the two day conference or TTXs**, and all new stories related to the conference should be coordinated with the National Press Office in OPA. Some presentations are more appropriate for public consumption. For example, the Associated Press wrote a story this week on the BAU presentation which is a story which needs to be coordinated through NPO and BAU.
- Changes and additions to the SIOC Active Shooter web site continue, including additional support materials for the conferences. If you have a new speaker, there are video presentations of each segment posted. Many other items are posted on the Resources section and virtually all those materials are available for law enforcement on the LEO.gov web site.
- We are aware some field office and their local departments are enhancing conferences through the presentation of local best practices and lessons learned. If you would like to share those materials with the AS team, we'll find ways to pass them along for use by others.

\* Please reach out with questions and concerns to me [REDACTED]

b6  
b7C

Thanks [REDACTED]

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



[REDACTED] RMD)(CON)

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Friday, September 06, 2013 9:26 AM  
**To:** [REDACTED]  
**Cc:** [REDACTED] DO) (FBI)  
**Subject:** FW: Active Shooter Initiative - 8.23.13 update --- UNCLASSIFIED

b6  
b7C  
  
b7E

Classification: UNCLASSIFIED  
=====

CLAs –

The email below was recently sent to the Active Shooter contacts in each field office.

I am forwarding it for your situational awareness in light of the EC I forwarded to you yesterday.

There will be one additional email from the Active Shooter program that will follow.

Thank you.

[REDACTED]  
SSA [REDACTED]  
Program Manager  
Campus Liaison Initiative

b6  
b7C  
b7E

[REDACTED]  
Counterterrorism Division - FBIHQ  
[REDACTED]

**From:** [REDACTED] (DM) (FBI)  
**Sent:** Thursday, August 22, 2013 7:27 PM  
**To:** [REDACTED] (DM) (FBI)  
**Cc:** [REDACTED] DO) (FBI)  
**Subject:** Active Shooter Initiative - 8.23.13 update --- UNCLASSIFIED

b6  
b7C

Classification: UNCLASSIFIED  
=====

Greetings,

This note provides an important update on the Active Shooter initiative and should be shared with field EM, as appropriate.

The Deputy Director was briefed recently on program progress, including the number and location of conferences and TTXs held to date. In a meeting with the IACP the same week, the DD, CIRG Assistant Director Yacone and Section Chief Combs were asked to post a calendar of upcoming conferences and tabletop exercises. Several chiefs and sheriffs spoke of the high quality and effectiveness of the conferences and their desire to increase participation. These law enforcement leaders asked that the dates be published so they also can advertise the effort. To meet this requirement, all field offices are asked to anticipate their planned events for the rest of the calendar year or beyond and provide



those dates back to Section Chief Combs (cc [redacted]) by COB Friday, Sept. 6. Conference dates will be posted for law enforcement access via LEO.gov.

b6  
b7C

Please make every effort to schedule conferences and TTXs in a variety of regions in your AOR. Many of these shooting incidents occur where small and medium sized departments do not have the resources and your field office can provide lessons learned at these events. Based on field requests, FY14 money is budgeted to pay for police executive hotel costs for the 2-day conferences when field offices need to provide travel to participants. Plans are to prioritize the funds based on requests in this schedule of conferences, as long as the budget plan remains intact.

Advance notification of scheduled events will also help FBIHQ forward handout materials (listed on SIOC Active Shooter web site) being printed with limited resources. Please send requests for handouts to [redacted], copied here.

b6  
b7C

Finally, several inquiries have come in about whether divisions will hold TTXs based on the college scenario. Please ensure campus public safety officers are invited to conferences and campus TTX events are scheduled at either FBI facilities or campus facilities.

Thanks for your continued support of this program.

[redacted]

b6  
b7C

*If you are no longer a POC for your FO or HQ Division, please reply to me only and let me know so I can take you off this list. Please provide the name of your replacement POC.*

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Thursday, September 05, 2013 2:18 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED] (O) (FBI)  
**Subject:** Sentinel Document Re: (U) Campus-Related Active Shooter Command Staff Seminars and Active Shooter Tabletop Exercises --- UNCLASSIFIED

b6  
b7C

b7E

Classification: UNCLASSIFIED

=====

Sent for Approval for RECORD//Sentinel Case [REDACTED]

CLAs –  
The FBI's Campus Liaison Initiative just put out an EC to the field with the following synopsis:

b7E

[REDACTED] see link below)

"Field Offices will invite campus public safety commanders to Active Shooter Command Staff Seminars and schedule Active Shooter Tabletop Exercises (TTX) using the specific scenario developed for institutes of higher education on CIRG's Active Shooter website. Campus public safety departments, if armed and sworn, will also be offered tactical ALERRT training."

The EC provides further information about how to accomplish the TTX and how to identify appropriate attendees. Please start scheduling Active Shooter Command Staff Seminars and TTXs for campus public safety in your division, in coordination with your Crisis Management Coordinator, Training Coordinator, seminar presenters, and executive management. Please document all seminars and TTXs to the CLI file.

Please encourage all armed and sworn campus police departments in your territory to attend ALERRT training. Contact the ALERRT Training Coordinator in your office if you need assistance with this.

The AS program will be sending an email to all SACs within the next week supporting this EC and providing them with an electronic copy.

As always, I'm available for any assistance you need with this venture.  
Thank you.

[REDACTED]  
SS [REDACTED]  
Program Manager  
Campus Liaison Initiative

b6  
b7C  
b7E

[REDACTED]  
Counterterrorism Division - FBIHQ  
[REDACTED]

The following document has been forwarded to you:

Title: (U) Campus-Related Active Shooter Command Staff Seminars and Active Shooter Tabletop Exercises

Synopsis: (U) Field Offices will invite campus public safety commanders to Active Shooter Command Staff Seminars and schedule Active Shooter Tabletop Exercises using the specific scenario developed for institutes of higher education on



CIRG's Active Shooter website. Campus public safety departments, if armed and sworn, will also be offered tactical ALERRT training.

Link to Document

b7E

=====

Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Wednesday, September 04, 2013 10:23 AM  
**To:** [REDACTED] (SE) (FBI)  
**Subject:** RE: UW Games --- UNCLASSIFIED

b6  
b7C

Classification: UNCLASSIFIED  
=====

[REDACTED]

b5

[REDACTED]

**From:** [REDACTED] SE) (FBI)  
**Sent:** Tuesday, September 03, 2013 4:49 PM  
**To:** [REDACTED] CTD) (FBI)  
**Subject:** UW Games --- UNCLASSIFIED

b6  
b7C

Classification: UNCLASSIFIED  
=====

[REDACTED]

b6  
b7C

Wanted to report that our assist on the UW home football game this weekend went really well. UWPD is grateful for our help and [REDACTED]

b7E

[REDACTED]

b5

Thanks for all your help  
=====

Classification: UNCLASSIFIED  
=====

Classification: UNCLASSIFIED



[REDACTED] RMD)(CON)

From: [REDACTED] CTD) (OGA)  
Sent: Tuesday, September 24, 2013 8:43 AM  
To: [REDACTED] SE) (FBI)  
Cc: [REDACTED] CTD) (FBI)  
Subject: [REDACTED] - UNCLASSIFIED//~~FOUO~~//LES

b6  
b7C  
b7E

Classification: UNCLASSIFIED//~~FOUO~~//LES

FYSA, the attached [REDACTED]

(U) [REDACTED]



b7E

[REDACTED]  
Special Agent

[REDACTED]  
detailed to the [REDACTED]  
[REDACTED]

b6  
b7C  
b7E

=====  
Classification: UNCLASSIFIED//~~FOUO~~//LES



[REDACTED] (RMD)(CON)

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Tuesday, November 12, 2013 6:43 AM  
**To:** [REDACTED]  
**Cc:** [REDACTED] DO) (FBI)  
**Subject:** Fw: Urgent Update for use of TR#s for Active Shooter conferences --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

CLAs --

Below you will find information regarding travel funds to support Active Shooter TTXs and Executive Seminars for campuses.

As you know, the Bureau has implemented TRIP, a new system for travel authorization and payment. As with all new Bureau systems, it will make the process much easier (insert heavy sarcasm).

Please read the information below carefully. I realize the process is awkward at best, but at least it provides funding for training campus public safety who wouldn't ordinarily receive this training.

If you have any questions about Active Shooter training or travel money, please contact [REDACTED] She is the CIRG manager for all campus public safety active shooter training.

Once again, thanks for your support of this worthwhile program.

[REDACTED]  
SSA [REDACTED]  
Program Manager  
Campus Liaison Initiative

b6  
b7C  
b7E

[REDACTED]  
Counterterrorism Division - FBIHQ  
[REDACTED]

**From:** [REDACTED] DM) (FBI)  
**Sent:** Tuesday, November 05, 2013 5:01 PM  
**To:** [REDACTED]  
**Subject:** Urgent Update for use of TR#s for Active Shooter conferences --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

Several Field Offices have already indicated a desire to use the FBIHQ, CIRG travel TR#s to support Active Shooter conferences in their AOR. As indicated in a pending EC (below) an in prior direction, FOs must send and EC describing the request for travel funds. In addition, in order to comply with Finance Division requirements, it is mandatory that the field office fill out the attached spreadsheet and forward to me as soon as practicable. Because the entire FBI is now utilizing UFMS, CIRG must transfer money to every field office that will be using the CIRG TR#s.





Please note that you will need to do two spreadsheets if you have FBI and non-FBI people traveling on different TR#s.

In each instance, the spreadsheet must indicate the anticipated cost estimate by traveler in order for CIRG to transfer the appropriate payment to your field office. Each office also has a duty to update the information if changes occur. For instance, if a traveler from one area of your AOR is no longer attending your school and being replaced by another, or you are sending different people to host a conference than first anticipated, [REDACTED] must be notified immediately via email so those supporting CIRG financial efforts can update FD records and ensure proper funds have been transferred. Your finance office will not be able to process TRIP requests until CIRG transfer funds to them. Please ensure this information is forwarded to your FO finance personnel. CIRG will perform the transfer to the field offices and will create one transfer with multiple lines for one TR number (instead of doing a transfer for each individual). Therefore, please ensure that your spreadsheet is complete to the best of your knowledge.

b6  
b7C

The CIRG TR# is not to be used for the ALERRT Active Shooter Training. The Training Division has a separate TR# for that travel and questions about management of that TR# should be addressed to [REDACTED] in PAU. FBIHQ is making every effort during this tight budget year to continue to support the field's Active Shooter initiatives. Highlights on use the TR# are listed below:

b6  
b7C

*As a reminder, in FY14, funding enhancements, based on field office requests, will provide support for:*

- FBI personnel travel to host conferences in FO AORs, and*
- hotel expenses only for non-FBI, law enforcement executives to attend FBI conferences. Funding is not for gas, cars, food or any other incidentals. Funds will be distributed based on the following circumstances:*

- Attendees - Hotel accommodations at the per diem rate will be allowed for no more than two nights for attendees if they must travel in the night before, and only if there is no conference being held within two hours of the law enforcement officials' department. In no circumstances may law enforcement personnel be offered hotel accommodations so they may travel away from headquarters city, for example, to attend a conference at an RA location.*
- Speakers - Standard DOJ per diem rules will apply and be permitted for one night only for FBI personnel presenting materials if the speaker is unable to drive back and forth to the conference in a work day. For example, if a speaker is on at 8 a.m., a hotel could be provided but the speaker must drive back after speaking and cannot stay over another night. To ensure consistency with the host department and location, however, one FBI employee coordinating the conference and one FBI executive may be allowed up to two but no more than three nights' accommodations depending on the travel distance needs and as authorized by the field office ASAC responsible for the Active Shooter program.*

*Travel funds were budgeted to support field requests with large AORs where concerns were expressed that distant small and medium departments might be left out of the training. Since this is being offered in respond to requests from offices with broad territories, scrutiny will be given to request authorization from more congested areas of the country.*

*In each instance, funding requests must be submitted via EC to SSA [REDACTED] SIOC, CIRG, and include details individuals requesting use of a TR#, their role in the event, and why they are unable to participate unless the funding is available. Travel funds for FBI personnel should use TR# 514N21522001. Travel funds for non-FBI personnel should use TR# 514N21522002.*

b6  
b7C

Please ensure this information is forwarded to appropriate personnel in your field office.



Regards

b6  
b7C

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

From: [REDACTED] CTD) (FBI)  
Sent: Thursday, October 24, 2013 8:49 AM  
To: [REDACTED]  
Subject: College Rx Initiative --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

CLAs -

Another resource:

[REDACTED]

## College Rx Initiative Targets Students

by [REDACTED] OPA

b7E

b6  
b7C

When SSA [REDACTED] supervised the applicant squad at Washington Field Office (WFO), he couldn't help but notice the number of young professionals turned down for jobs with the FBI due to prescription drug abuse and misuse. Today, SSA [REDACTED] supervises Health Care Fraud Squad CR-19, Criminal Investigative Division (CID), at WFO, and he's watched statistics on prescription abuse steadily increase. In December 2011, the University of Michigan's Monitoring the Future study found that, among 12<sup>th</sup> graders, prescription drugs are being abused at a rate second only to the use of marijuana.

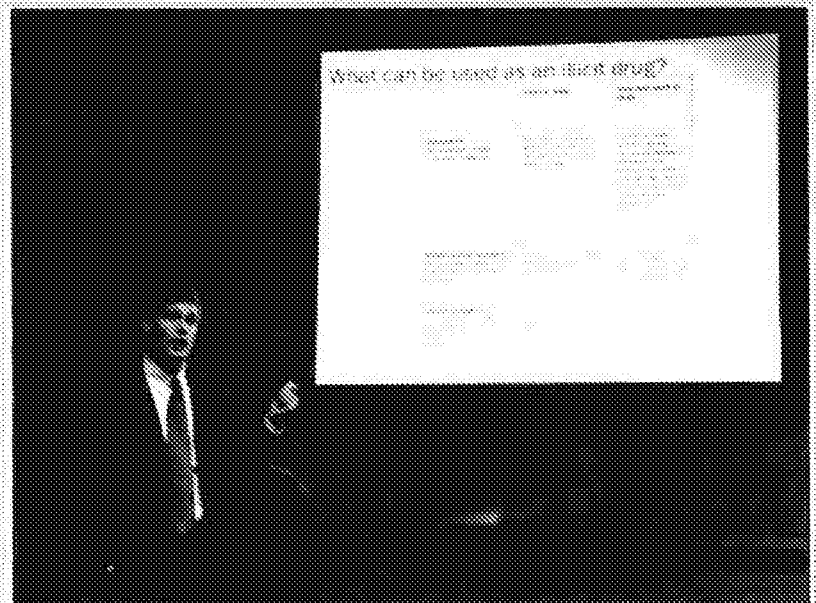
"In some cases, it's recreational. But a lot of it is pressure from the students trying to succeed through college," he said.

Under SSA [REDACTED] direction, an intern with CR-19 this summer- [REDACTED]

extensively researched these numbers. She found a 2010 study by the National Institute on Drug Abuse that said 7 million Americans reported using prescription drugs for nonmedical purposes. A report by the Institute in 2011 found full-time college students between ages 18 and 22 are twice as likely to use a stimulant for non-medical reasons than those who are in college part time or not at all.

Her research culminated with the creation of a PowerPoint presentation called the College Rx Initiative, designed for college freshmen audiences and their senior class mentors. The Initiative highlights the health and crime dangers associated with prescription medications. It also points out the irony in how abusing the drugs to make good grades could hurt them in obtaining positions with government and private industry employers.

The PowerPoint is available to all field offices. SSA [REDACTED] hopes other special agents will contact student affairs departments at colleges and universities in their own areas of responsibility to schedule



SA [REDACTED] speaking at Georgetown University

b6  
b7C

b6  
b7C



presentations. He said it works best if it is shown during orientation to the freshmen class and to seniors assigned to mentor them.

So far, students at Georgetown, American, and Catholic universities have attended College Rx Initiative presentations.

"They were very receptive," said SA [REDACTED] CR-19, WFO, who gave a presentation at Georgetown University. "I think a lot of them were surprised at the restrictions the government can put on past drug use." b6 b7C

He said information about the effects that prescription drug abuse and misuse can have on their future careers seemed to resonate more with his audience than warnings about health risks and jail sentences. Some, he said, were just surprised to find out it was a crime.

"Kids don't see them the same as street drugs," SA [REDACTED] said. "It was a little eye-opening to them that handing out Adderall (a drug commonly used to treat ADHD) to friends before an exam could be considered drug dealing."

Studies conducted by the National Institutes of Health back this up. In one interview, a 20-year-old said, "I think prescription drugs sound safer." And a 19-year-old told researchers, "Some people think prescription drugs aren't as harmful as street drugs because they are made by somebody who knows what they are doing...They weren't made in somebody's house and they were tested and FDA approved." The College Rx Initiative illustrates how untrue this belief really is. A National Institute on Drug Abuse study reports that in 2007, the number of overdose deaths from prescription opioids outnumbered deaths from heroin and cocaine combined. Misuse and abuse of medications can cause organ damage, heart attack, addiction, and even death.

And unless students become educated about the repercussions, all of these numbers, SSA [REDACTED] said, are predicted to go up.

If you would like a copy of the College Rx Initiative PowerPoint presentation to use in your area of responsibility, click here. Or, for more information, email SSA [REDACTED] at [REDACTED] b6 b7C

=====  
Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

b6  
b7C

From: [REDACTED] (CTD) (FBI)  
Sent: Friday, October 04, 2013 9:00 AM  
To: [REDACTED]  
Subject: FW: Government Funding Lapse - Affect on Active Shooter activities --- UNCLASSIFIED

b7E

Classification: UNCLASSIFIED

=====

Sent for Approval for RECORD//Sentinel Case [REDACTED]

b7E

From: [REDACTED] (DM) (FBI)  
Sent: Thursday, October 03, 2013 3:52 PM  
To: [REDACTED]  
Subject: Government Funding Lapse - Affect on Active Shooter activities --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED

=====

Note to POCs on the Active Shooter Initiative:

Good afternoon -- We have had a few inquiries about how the government shutdown affect the field Active Shooter initiatives and funding matters. Please be aware of the following guidance from the Finance Division:

***Training, Conferences, and Other Events:** Training of current employees, even those who are excepted for emergency reasons, should be cancelled or delayed, except in the rare circumstance when immediate training is necessary to protect human life or property. Those excepted employees whose training has been cancelled/delayed must report to their official duty stations. Training of state and local law enforcement officers should be cancelled during a lapse of appropriations. Training, conferences, or other events where the FBI is reimbursed the travel cost by a non-Federal source (through the FD-934 process) should be cancelled during the lapse of appropriations. -- FD guidance*

We are still awaiting some information, however, based on conversations with TD and FD please be advised:

**1. ALERRT Training**

No FBI Tactical Instructors are permitted to participate in ALERRT training for state, local, tribal and campus law enforcement. ALERRT will continue to train with its own instructors and funding provided by DOJ and FBI in FY13.

**2. Conferences and TTXs** - FD is in the process of determining whether the Conferences and TTXs can be held if we remain in this lapse of appropriations. We have asked for an exception based on the fact that these events affect law enforcement/first responders attendees with regard to " jobs necessary for the safety of human life or protection of property." We have also asked whether the FY14 TR# for expenses can be used during this time. We'll let you know as soon as we hear.

We have secured FY14 funding to assist field offices in limited ways with travel expenses on future training and conference. An EC to the field will be forthcoming detailing FY14 goals and objectives for the Active Shooter Initiative. This is our current list of conferences and TTXs scheduled. Please keep us updated:



Field Office	Date	Location
Cincinnati	Oct 16-17	Sinclair Community College (Dayton, OH)
Richmond	Oct 16-17	Southwest Virginia Higher Education Center (Abington, VA)
Mobile	Oct 24-25	Montgomery PD firing range
Columbia	Oct 21-22	Connon Center, Greer, SC
Atlanta	Oct 24-25	Georgia Regents University (Augusta, GA)
Phoenix	Nov 5-6	Flagstaff RA
New Orleans	Nov 13-14	Alexandria RA
Omaha	Nov 14-15	Iowa Law Enforcement Academy (Johnston, IA)
Memphis	Nov 14 (TTX)	Nashville, TN
Atlanta	Dec 17-18	Georgia Southern University (Statesboro, GA)
Phoenix	Mar 4-5, 2014	Tuscon RA
Phoenix	Apr 2-3, 2014	Yuma RA

Thanks,

[REDACTED]  
Special Assistant to CCRSB EAD Richard McFeely  
[REDACTED]

b6  
b7c

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

From: [REDACTED] (CTD) (FBI)  
Sent: Thursday, September 26, 2013 12:21 PM  
To: [REDACTED] (SE) (FBI)  
Cc: [REDACTED] (CTD) (OGA) [REDACTED] (CIRG) (FBI)  
Subject: FV [REDACTED] - UNCLASSIFIED//~~FOUO~~

b6  
b7C  
b7E

Classification: UNCLASSIFIED//~~FOUO~~

=====

TRANSITORY RECORD

[REDACTED]  
FYSA  
Just wanted to ensure you were aware of this. This is the link to the [REDACTED] the text is copied below.

b6  
b7C  
b7E

[REDACTED]  
It appears your NCAVC Coordinator in Seattle is already engaged.  
You might need to make a trip to the NW to provide assistance. ;)

b6  
b7C  
b7E

[REDACTED]  
SSA [REDACTED]  
Program Manager  
Campus Liaison Initiative

[REDACTED]  
Counterterrorism Division - FBIHQ  
[REDACTED]

From: [REDACTED] (CTD) (OGA)  
Sent: Thursday, September 26, 2013 11:43 AM  
To: [REDACTED] (CTD) (FBI)  
Cc: [REDACTED] (CTD) (OGA) [REDACTED] (CTD)(FBI)  
Subject: [REDACTED] - UNCLASSIFIED//~~FOUO~~

b6  
b7C  
b7E

Classification: UNCLASSIFIED//~~FOUO~~

=====

TRANSITORY RECORD

[REDACTED]  
Campus Police involved in this matter

b6  
b7C

[REDACTED]

b6  
b7C  
b7E



[Redacted]

[Redacted]

Senior Special Agent

[Redacted]

Desk [Redacted]

BB: [Redacted]

[Redacted] (U//FOUO) [Redacted]

(U//FOUO) [Redacted]

b6  
b7C  
b7E

b6  
b7C  
b7E

[Redacted]

b6  
b7C  
b7E

[Redacted]

b6  
b7C  
b7E

[Redacted]

b6  
b7C  
b7E

[Redacted]

b6  
b7C  
b7E

[Redacted]

[Redacted]



[Redacted]

b6  
b7C  
b7E

Status: Open

Type 1/Type 2

Precedence: Routine

Incident Suspicious

Type: Activity

Activity

Type:

[Redacted]

b7E

Observed:

[Redacted]

Origin

Agency: FBI

Receipt

Method: In Person

Reported

By:

SA [Redacted]  
[Redacted]

b6  
b7C  
b7E

[Redacted]

Assigned

Office:

Seattle

Assigned

Squad:

SWRA

Assigned

User:

[Redacted]

Incident

Creator:

[Redacted]

Incident

Owner:

[Redacted]

Incident

Due Date:

[Redacted]

05:17:45

b6  
b7C  
b7E

=====  
Classification: UNCLASSIFIED//~~FOUO~~

=====  
Classification: UNCLASSIFIED//~~FOUO~~



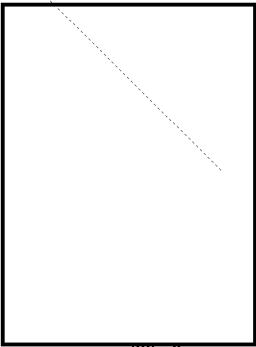
b7E

~~SECRET~~



(S)

b1  
b3



DD Question

[Redacted]

4\_13 -

b7E



(U) FBI Initiatives to Address Threats

[Redacted]

b1  
b3

Division	Description
CTD	(U//FOUO) Campus Liaison Initiative - Campus Liaison Agents in every field office work with Public Safety to increase information sharing and provide training to identify and mitigate
(S) CTD	[Redacted]
CTD	(U//FOUO) Civil Aviation Security Program - FBI Airport Liaison Agents are assigned to all regulated airports and conduct liaison through [Redacted]
CD	(U//FOUO) Academic Alliance - Coordinators collaborate with university leaders, including the more than 20 universities represented on the FBI's National Security Higher Education Board, including Arizona State University
(S) CD	[Redacted]
CD	
CD	
CD	
CyD	
WMDD	(U//FOUO) FBI Academic Partnership Initiative - Weapons of Mass Destruction Coordinate academic security workshops with science programs involving all levels of the university which utilize a multi-sector approach to develop and institute mechanisms to mitigate internal and external risks and threats (international and domestic terrorism, cyber security, protection of intellectual property/proprietary information, dual-use research, short place violence, security challenges with the rapid advances in research and technology innovations, and insider threat mitigation) and establish notification systems for suspicious behaviors and activities

b1  
b3

b7E

b1  
b3

From [Redacted] (CTD)(FBI)

Sent: Monday, June 17, 2013 3:41 PM

To [Redacted] (CTD)(FBI)

Cc [Redacted] (CTD) (FBI); [Redacted] (CTD)(FBI); [Redacted] (CTD) (FBI)

Subject: RE: Need new Coordination for AD McCabe/DD Joyce tasking on [Redacted] -- ~~SECRET//NOFORN~~

b6  
b7C

b7E



~~SECRET~~

Classification: ~~SECRET//NOFORN~~

~~Classified By: D88B69S71~~  
~~Derived From: FBI IAS-20090731~~  
~~Declassify On: 20381231~~  
=====

(S) The only [redacted] from the list we compiled a few weeks ago. The rest sound more [redacted] related.

b1  
b3 b7E

[redacted] MPA  
[redacted] Front Office  
Non-Secure [redacted]  
Secure: [redacted]

b6  
b7C

b7E

From: [redacted] (CTD)(FBI)  
Sent: Monday, June 17, 2013 3:38 PM  
To: [redacted] (CTD)(FBI)  
Cc: [redacted] (CTD) (FBI); [redacted] (CTD)(FBI); [redacted] (CTD) (FBI)  
Subject: RE: Need new Coordination for AD McCabe/DD Joyce tasking on [redacted] -- ~~SECRET//NOFORN~~

b6  
b7C

b7E

Classification: ~~SECRET//NOFORN~~

~~Classified By: J42J85T71~~  
~~Derived From: FBI IAS-20090731~~  
~~Declassify On: 20381231~~  
=====

Any of them related to [redacted]

b7E

From: [redacted] (CTD)(FBI)  
Sent: Monday, June 17, 2013 3:37 PM  
To: [redacted] (CTD)(FBI)  
Cc: [redacted] (CTD) (FBI); [redacted] (CTD)(FBI); [redacted] (CTD) (FBI)  
Subject: RE: Need new Coordination for AD McCabe/DD Joyce tasking on [redacted] -- ~~SECRET//NOFORN~~

b6  
b7C

b7E

Classification: ~~SECRET//NOFORN~~

~~Classified By: D88B69S71~~  
~~Derived From: FBI IAS-20090731~~  
~~Declassify On: 20381231~~  
=====

These are really the only initiatives they want to know about [redacted] has 4 full pages of initiatives...

b7E

[redacted] MPA  
[redacted] Front Office

b6  
b7C

~~SECRET~~



~~SECRET~~

Non-Secure: [redacted]  
Secure: [redacted]

b6  
b7C  
b7E

**From:** [redacted] (CTD)(FBI)  
**Sent:** Monday, June 17, 2013 3:28 PM  
**To:** [redacted] (CTD)(FBI)  
**Cc:** [redacted] (CTD) (FBI); [redacted] (CTD)(FBI); [redacted] (CTD) (FBI)  
**Subject:** FW: Need new Coordination for AD McCabe/DD Joyce tasking on [redacted] -- ~~SECRET//NOFORN~~

b6  
b7C  
b7E

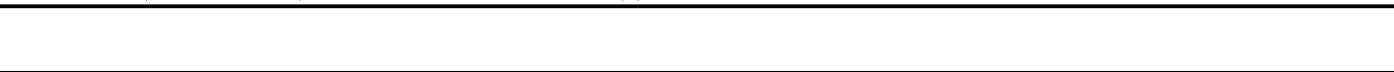
Classification: ~~SECRET//NOFORN~~

Classified By: J42J85T71  
Derived From: FBI IAS-20090731  
Declassify On: 20381231  
=====

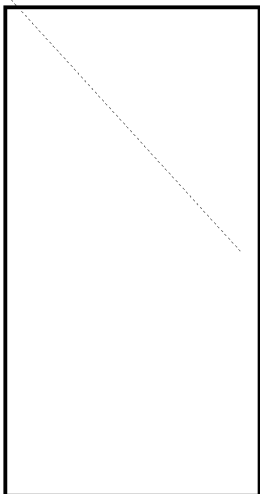
[redacted] please see below. Global is asking for CTD initiatives for the following. If this is something that you have already collected, I don't want to task this out again. Currently, only the following are listed in the attachment. I am not sure if there anything that you collected that could be added to the chart below or if that is all that we have to address this issue.

b6  
b7C

<< OLE Object: Picture (Device Independent Bitmap) >>



b7E



b1  
b3

<< File: DD Question Students 4\_4\_13 - Dissemination version.docx >>

**From:** [redacted] (CTD) (FBI)  
**Sent:** Monday, June 17, 2013 3:21 PM  
**To:** [redacted] (CTD)(FBI)  
**Cc:** [redacted] (CTD)(FBI); [redacted] (DI) (FBI); [redacted] (CTD) (FBI)  
**Subject:** RE: Need new Coordination for AD McCabe/DD Joyce tasking on [redacted] -- ~~SECRET//NOFORN~~

b6  
b7C  
b7E

Classification: ~~SECRET//NOFORN~~

~~SECRET~~



~~SECRET~~

Classified By: C22W37B52  
Derived From: FBI IAS-20090731  
Declassify On: 20381231  
=====

Yup.

**From:** [redacted] (CTD)(FBI)  
**Sent:** Monday, June 17, 2013 3:18 PM  
**To:** [redacted] (CTD) (FBI)  
**Cc:** [redacted] (CTD)(FBI); [redacted] (DI) (FBI); [redacted] (CTD) (FBI)  
**Subject:** FW: Need new Coordination for AD McCabe/DD Joyce tasking on [redacted] --- SECRET//NOFORN  
**Importance:** High

b6  
b7C

b7E

Classification: ~~SECRET//NOFORN~~

Classified By: J42J85T71  
Derived From: FBI IAS-20090731  
Declassify On: 20381231  
=====

[redacted] is this the tasking that you are working with [redacted] on?

b6  
b7C

**From:** [redacted] (DI) (FBI)  
**Sent:** Monday, June 17, 2013 3:16 PM  
**To:** [redacted] (CD) (FBI); [redacted] (CID) (FBI); [redacted] (CID) (FBI); [redacted] (CTD)(FBI); [redacted] (DI) (FBI); [redacted] (CYD) (FBI); [redacted] (CYD) (FBI); [redacted] (CYD) (FBI); [redacted] (OIO) (FBI); [redacted] (MD) (FBI); [redacted] (OIO)(FBI); [redacted] (DI)(FBI); [redacted] (DI)(FBI); [redacted] (DI)(FBI)  
**Cc:** [redacted] (DI) (FBI); [redacted] (DI)(FBI)  
**Subject:** FW: Need new Coordination for AD McCabe/DD Joyce tasking on [redacted] --- SECRET//NOFORN  
**Importance:** High

b6  
b7C  
b7E

b7E

Classification: ~~SECRET//NOFORN~~

Classified By: F26M99K70  
Derived From: FBI IAS-20090731  
Declassify On: 20381231  
=====

Colleagues,

<< File: DD Question Students 4\_4\_13 - Dissemination version.docx >>

The attached product was presented to FBI senior management in late February. Last week, DD Joyce brought the issue up again with a list of [redacted] he's interested in. Initially, CTD took lead on the tasking but has passed it to GIS. They're expecting a response to AD McCabe and DD Joyce "mid to late" this week.

b7E

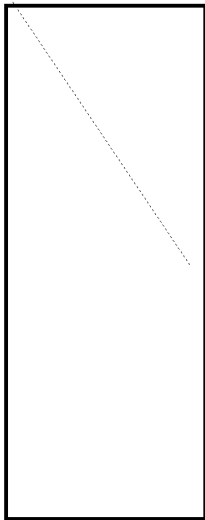
b7E

~~SECRET~~



~~SECRET~~

(S)



b1  
b3

Please return your responses to everyone in the Cc... line of this email NLT 4pm on 18 June 2013.

Thanks!

SIA [redacted]  
DI Coordination Cell  
Desk [redacted]

b6  
b7C

"You can't defend. You can't prevent. The only thing you can do is detect and respond."  
Bruce Schneier

=====  
Classification: ~~SECRET//NOFORN~~

=====  
Classification: ~~SECRET//NOFORN~~

=====  
Classification: ~~SECRET//NOFORN~~

=====  
Classification: ~~SECRET//NOFORN~~

=====  
Classification: ~~SECRET//NOFORN~~

=====  
Classification: ~~SECRET//NOFORN~~

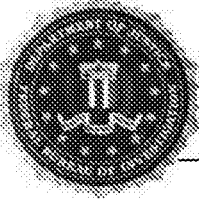
=====  
Classification: ~~SECRET//NOFORN~~

=====  
Classification: ~~SECRET//NOFORN~~

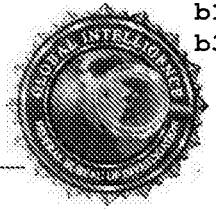
=====  
Classification: ~~SECRET//NOFORN~~

~~SECRET~~





(S) ~~SECRET//NOFORN~~  
FOR INTERNAL USE ONLY



b1  
b3

*Directorate of Intelligence/Global Intelligence Section*

(U//FOUO) [redacted] Exploitation and Mitigation

b1  
b3  
b7E

(S//NF)

(S)

X

(U) Counterterrorism Threats

(S)

X

(S//NF)

b1  
b3

(S)

X

b1  
b3

<sup>1</sup> (U//FOUO) This number is provided by [redacted] data from 2011, which was the last complete year's worth of data when this project began.

b7E

(S) ~~SECRET//NOFORN~~  
FOR INTERNAL USE ONLY

FBI INFO.  
CLASSIFIED BY NSICG/F76M45K62  
REASON: 1.4 (C, D)  
DECLASSIFY ON: 04-01-2040  
DATE: 04-01-2015

b1  
b3



(S)

SECRET//NOFORN  
FOR INTERNAL USE ONLY

b1  
b3

### (U) Counterintelligence Threats

(S//NF

b1  
b3

### (U) Weapons of Mass Destruction Threats

(S//NF

b1  
b3

### (U) Criminal Threats

(U//FOUO) The criminal threat includes organized crime groups attempting to use student visas to help illegal aliens enter the United States or to get other forms of identification to conduct financial fraud.

### (U) Potential Vulnerabilities in Addressing Threats

(S//NF

b1  
b3

(S)

SECRET//NOFORN  
FOR INTERNAL USE ONLY

b1  
b3



b1  
b3

(U) FBI Initiatives to Address Threats

(S//NF) [redacted]

b1  
b3

[redacted]

Division	Description
CTD	(U//NF) <del>CTD</del> Campus Liaison Initiative - Campus Liaison Agents in every field office work with Campus Security Authorities to develop and implement security plans for students and visitors to campus.
(S) CTD	[redacted]
CTD	(U//NF) <del>CTD</del> Civil Aviation Security Program - FBI Airport Liaison Agents are assigned to all 446 TSA regulated airports and conduct liaison through CTD [redacted]
CD	(U//NF) <del>CD</del> Academic Alliance - Coordinators collaborate with university leaders, including those at the more than 20 universities represented on the FBI's National Security Higher Education Advisory Board, including Rutgers State University.
CD	[redacted]
(S) CD	
CD	
CD	
CyD	
WMDO	(U//NF) <del>WMDO</del> FBI Academic Partnership Initiative - Weapons of Mass Destruction Coordinators conduct academic security workshops with science programs involving all levels of the university system which utilize a multi-sector approach to develop and institute mechanisms to mitigate internal and external risks and threats (international and domestic terrorism, cyber security, protection of intellectual property, proprietary information, dual-use research, work place violence, security challenges with the rapid advances in research and technology innovations, and insider threat infection and establish notification systems for suspicious behaviors and activities.

b1  
b3

b7E

b1  
b3

b1  
b3



(U) Appendix A: Maps

(S)



b1  
b3



(U) Appendix E [redacted]

b7E

\* (U) Denotes members of the National Security Higher Education Advisory Board (NSHEAB)

- (U//~~FOUO~~) Note: [redacted]  
[redacted]

(S)

b1  
b3



[REDACTED] RMD)(CON)

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Wednesday, August 28, 2013 10:49 AM  
**To:** [REDACTED] (SE) (FBI)  
**Subject:** FW: [REDACTED] - UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

I wanted to ensure you were looped in.

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Wednesday, August 28, 2013 10:34 AM  
**To:** [REDACTED] CTD) (OGA)  
**Cc:** [REDACTED] CTD) (FBI)  
**Subject:** FW: [REDACTED] -- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

FYI -- we have no indication this is animal rights extremism related, but thought you would want to know as it impacts WSU. Thanks.

[REDACTED]  
Intelligence Analyst

[REDACTED]  
Animal Rights/Environmental Extremism  
Anarchist Extremism

b6  
b7C  
b7E

**From:** [REDACTED] CTD)(FBI)  
**Sent:** Monday, August 26, 2013 3:00 PM  
**To:** [REDACTED] CTD) (FBI)  
**Subject:** FW: [REDACTED] --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

Fyi -- just cause of the mice reference

**From:** [REDACTED] SE) (FBI)  
**Sent:** Monday, August 26, 2013 2:05 PM  
**To:** [REDACTED] WMD) (FBI); [REDACTED] (SE)(FBI); [REDACTED] (SE) (FBI); [REDACTED]  
[REDACTED] (SE) (FBI); [REDACTED] E) (FBI)  
**Cc:** [REDACTED] CTD)(FBI); [REDACTED] CTD) (FBI); [REDACTED] (SE)(FBI); [REDACTED]  
[REDACTED] (SE)(FBI); [REDACTED] (SE) (FBI); [REDACTED] (SE)(FBI); [REDACTED]

b6  
b7C



(SE)(FBI) [redacted] (SE)(FBI) [redacted] (WMD) (FBI) [redacted] (E)(FBI) [redacted]

b6  
b7C  
b7E

(SE) (OGA)  
**Subject:** RE: [redacted] -- UNCLASSIFIED

Classification: UNCLASSIFIED

=====

Morning [redacted] we are in the process of opening a [redacted]  
[redacted]

b6  
b7C  
b7E

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

b6  
b7C  
b7E

We plan to take custody of the materials tomorrow (Tuesday, 8/27/2013), and will need to consider a TCE prior to handling. Please see attached:



[redacted]

b7E

Thank you.

b6  
b7C

[redacted]  
Supervisory Senior Resident Agent  
Eastern Washington  
[redacted] (direct)  
[redacted] (mobile)  
509.458.8110 (fax)

[redacted]  
1116 W. Riverside Ave.  
Suite 200  
Spokane, WA 99201

**From:** [redacted] (WMD) (FBI)  
**Sent:** Monday, August 26, 2013 9:19 AM  
**To:** [redacted] (SE) (FBI); [redacted] (SE)(FBI); [redacted] (SE) (FBI)  
**Subject:** [redacted] -- UNCLASSIFIED

b6  
b7C

b7E

Classification: UNCLASSIFIED

=====



Hello all,

Few questions regarding the [redacted]

1. Any other new updates yet?

2. Do you anticipate opening a [redacted]

b7E

Thank You

SSA [redacted]

WMDD-OIU

b6  
b7C

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



# Seattle Division Spokane RA

[REDACTED]

[REDACTED]

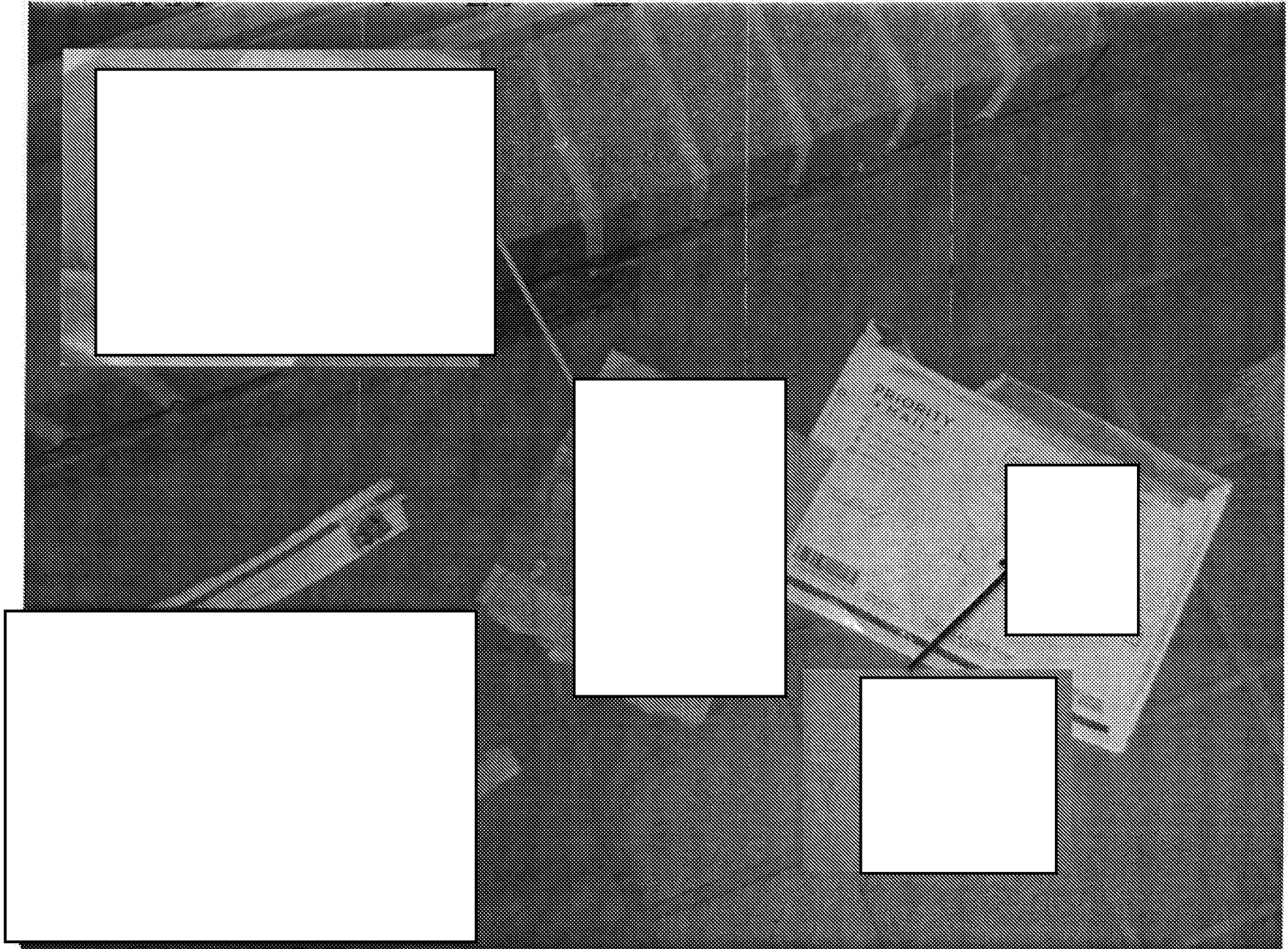
b6  
b7C  
b7E

[REDACTED]

[REDACTED]

b7E





b6  
b7C  
b7E



[REDACTED] (RMD)(CON)

From: [REDACTED] CTD) (OGA)  
Sent: Wednesday, August 28, 2013 8:53 AM  
To: [REDACTED] (SE) (FBI)  
Cc: [REDACTED] CTD) (FBI) [REDACTED] CTD) (FBI)  
Subject: [REDACTED] UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED

=====  
FYSA, the attached [REDACTED] (U) [REDACTED]

b7E

[REDACTED]  
(U) [REDACTED]  
[REDACTED]

b7E

[REDACTED]

[REDACTED]

Special Agent

[REDACTED]

b6  
b7C  
b7E

=====  
Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

b6  
b7C

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Monday, July 29, 2013 1:33 PM  
**To:** [REDACTED]  
**Subject:** FW: CLI Response to Field Division Inspection Inquiries --- UNCLASSIFIED

b7E

Classification: UNCLASSIFIED  
=====

Below is an example of what one of your fellow CLAs is using to report his activity during file reviews and on a quarterly basis.

I'm sending it out as a pony in case any of the rest of you would like to utilize this format. It is similar to the one used by [REDACTED] cases.

b7E

**From:** [REDACTED] (IP) (FBI)  
**Sent:** Thursday, July 25, 2013 11:10 AM  
**To:** [REDACTED] CTD) (FBI)  
**Subject:** RE: CLI Response to Field Division Inspection Inquiries --- UNCLASSIFIED

b6  
b7C

Classification: UNCLASSIFIED  
=====

H [REDACTED]

b6  
b7C

Just an example of what we do here in Indy under the guidance of one [REDACTED] At our quarterly file reviews I provide him with a case progress report (also known as a baseball card) that summarizes our CLI outreach and activities for the quarter. I am attaching an example from last quarter. It is a quick 2 page snapshot of Indy's CLI program covering the period April 1, 2013 through June 30, 2013. It works well here and may be helpful to other CLAs. I will begin to upload these to the HQ CLI file quarterly.



[REDACTED]  
Campus Liaison....

b7E

Good times,  
[REDACTED]

SA [REDACTED]  
Indianapolis [REDACTED]  
[REDACTED] desk  
[REDACTED] 88  
[REDACTED]

b6  
b7C  
b7E

**From:** [REDACTED] (CTD) (FBI)  
**Sent:** Thursday, July 25, 2013 10:59 AM

b6  
b7C



To [redacted]

Subject: CLI Response to Field Division Inspection Inquiries --- UNCLASSIFIED

b7E

Classification: UNCLASSIFIED

CLAs --

The Inspection Division has devised a new inspection process for field divisions. I don't know much about it, except whenever a field office is scheduled for an inspection, I receive a request to respond to questions as they pertain to the CLI as part of the overall CTD response to the Inspection Division.

To accurately summarize what the CLI program in a field office has accomplished, in Sentinel I pull all the documents written by that field office serialized to the CLI case file [redacted] during the inspection time period.

b7E

I want to ensure you are all aware of this process to ensure you have the opportunity to document on a regular basis all the hard work you do. It's frustrating for me when I receive a request and go to pull the documents, but there is nothing there even though I know the CLA in that division has done good work.

I have attached two documents below. The first is the series of inspection questions for which CTD is requested to provide responses.

The second document is an example of a CLI response I provided. It is actually an unusual example because it was not written by me. I was on official travel last week, and received the inspection tasking on my BB. I was unable to check Sentinel on the road, so I reached out to the CLA in the field office that was being asked for in last week's tasking, and asked that he provide a summary for me. He provided the attached which I thought was a good example of what Inspection Division and his field office management would want to know about the program. Hopefully when I am doing the research for these taskings, this is the type of information that is included in documents in the CLI case file.

Once again, thanks for all you do.

[redacted]  
SSA [redacted]  
Program Manager  
Campus Liaison Initiative

b6  
b7C  
b7E

[redacted]  
Counterterrorism Division - FBIHQ  
[redacted]

<< File: Inspection for field offices template 7-17-2013.docx >> << File: Inspection for field offices CLI response example 7-13.docx >>

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



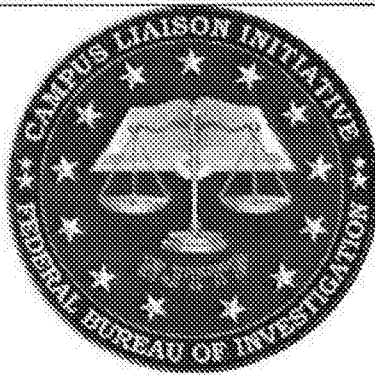
-----

Classification: UNCLASSIFIED



**CAMPUS LIAISON INITIATIVE** [REDACTED]

b7E

<u>CTD Points of Contact:</u>  SSA [REDACTED] [REDACTED]		<u>Field Office Points of Contact</u>  SSA [REDACTED] [REDACTED] SA [REDACTED] [REDACTED]
---	--	--

b6  
b7C

**Predication:** [REDACTED] established the Campus Liaison Initiative (CLI) designed to assist the field divisions in establishing enhanced liaison with college and university campuses in an effort to prevent terrorist incidents, raise awareness of the terrorist threat to campuses, and illustrate the role and mission of the [REDACTED]  
[REDACTED]

b7E

**Summary:** The CLI is an opportunity for the CLA to liaise with university and collegiate personnel regarding issues that affect campus throughout the state. The CLA can brief administration, law enforcement, faculty, or students on issues that are pertinent to those groups. It also is a way of promoting a working relationship with the local [REDACTED]  
[REDACTED]

b7E

**Current Information:**

On 04/08/2013, information was disseminated regarding a No Drone Action Day to members of Indiana Campus Law Enforcement Administrators (INCLEA). The action day was scheduled to take place between April 16-18.

On 04/08/2013, information was disseminated regarding an FBI Active Shooter Conference to members of Indiana Campus Law Enforcement Administrators (INCLEA). The conference took place April 23-24 and was open to campus law enforcement/public safety personnel.

On 04/12/2013, Campus Liaison Agent attended the quarterly Indiana Campus Law enforcement Administrators (INCLEA) meeting at Anderson University. Discussed at the meeting were current happenings at campus/universities throughout the state. Special focus was paid to the summer Campus Protection Officer course and the curriculum to be taught. CLA spoke to recent distributions to the INCLEA list-serve account regarding the No Drone Action Day and the FBI Active Shooter Training later in April at the Indiana War Memorial.



On 04/16/2013, a Joint Intelligence Bulletin was disseminated pertaining to the Boston Marathon bombings to members of Indiana Campus Law Enforcement Administrators (INCLEA).

On April 23-24, 2013, CLA attended the Active Shooter Conference hosted by FBI Indianapolis. This conference included presentations on pre-incident indicators, victim/witness services, media relations, command posts, bombs/IEDs, evidence, and department training. The conference concluded with a TTX on an active shooter scenario. In attendance at the conference were state/local/federal law enforcement/fire/ems and higher educational institutions from across Indiana.

On 04/23/2013 a basic FBI presentation was given to 93 students at Indiana State University attending an Introduction to Criminal Justice class.

On 04/29/2013, a Joint Intelligence Bulletin was disseminated regarding "University Laboratories Remain Vulnerable to Theft of Chemicals and Equipment for Potential Criminal and Extremist Purposes" to members of Indiana Campus Law Enforcement Administrators (INCLEA).

On 05/06/2013 [REDACTED] members of Indiana Campus Law Enforcement Administrators (INCLEA). This was done for awareness during upcoming commencement exercises.

b7E

On 05/16/2013, training was provided to the University of Southern Indiana's Campus Protection Officers. The presentation included an overview of the FBI JTTF and Campus Liaison Initiative along with a detailed discussion of Domestic and International Terrorism related to universities. Approximately 15 campus officer were in attendance for the 90 minutes training.

On 05/16/2013, a video and brochure on chemical security was given to Butler University Police Department Assistant Chief [REDACTED]. The WMDD/Chemical Countermeasures Unit created a chemical security outreach video with a focus on laboratory security awareness, specifically for colleges and universities. This video, entitled *Chemical Indicators*, was recently mentioned in an Intelligence Bulletin that was distributed on April 24, 2013, which references the general vulnerability of university chemical inventories to exploitation.

b6  
b7C

On 06/13/2013 A two hour block of instruction was given to the 39 cadets of the Indiana University Police Academy, who represent the Bloomington, Indianapolis, New Albany, Richmond, Kokomo and Gary campuses. The presentation was an overview of the FBI, JTTF, general CT goals and protocols and a request to contact the FBI with any information that may assist our mission when these officers begin patrol duties around the country.

On 06/14/2013, an information report was disseminated regarding a [REDACTED]  
[REDACTED] This

b7E



report was distributed to the Indiana Campus Law Enforcement Administrators (INCLEA) for awareness.

On 06/18/2013, Carmel Police Department facilitated an "Operation-Active Shooter" Tabletop Exercise at Carmel High School. This exercise was a discussion based incident and included representatives from Carmel Fire Department, Carmel High School (Staff) and Carmel Police Department. Role players and observers worked in groups to formulate plans and discuss pre-determined questions regarding the incident. [ ] SSA attended this event.

b7E

**Upcoming/Ongoing Information:**

- CLA is maintaining liaison contacts with Indiana campus law enforcement and disseminating relevant information as it is obtained
- CLA is maintaining situational awareness and providing guidance on investigations involving Indiana Universities and students
- CLA is working with Indianapolis Domain Coordinator on Campus issues
- CLA is attending INCLEA meetings on a quarterly basis (next meeting 04/12/2013).

07/18/2013



[REDACTED] (RMD)(CON)

From: [REDACTED] CTD) (FBI)  
Sent: Thursday, July 25, 2013 10:59 AM  
To: [REDACTED]  
Subject: CLI Response to Field Division Inspection inquiries --- UNCLASSIFIED

b6  
b7C  
  
b7E

Follow Up Flag: Follow up  
Flag Status: Flagged

Classification: UNCLASSIFIED  
=====

CLAs –  
The Inspection Division has devised a new inspection process for field divisions. I don't know much about it, except whenever a field office is scheduled for an inspection, I receive a request to respond to questions as they pertain to the CLI as part of the overall CTD response to the Inspection Division.

To accurately summarize what the CLI program in a field office has accomplished, in Sentinel I pull all the documents written by that field office serialized to the CLI case file [REDACTED] during the inspection time period.

b7E

I want to ensure you are all aware of this process to ensure you have the opportunity to document on a regular basis all the hard work you do. It's frustrating for me when I receive a request and go to pull the documents, but there is nothing there even though I know the CLA in that division has done good work.

I have attached two documents below. The first is the series of inspection questions for which CTD is requested to provide responses.

The second document is an example of a CLI response I provided. It is actually an unusual example because it was not written by me. I was on official travel last week, and received the inspection tasking on my BB. I was unable to check Sentinel on the road, so I reached out to the CLA in the field office that was being asked for in last week's tasking, and asked that he provide a summary for me. He provided the attached which I thought was a good example of what Inspection Division and his field office management would want to know about the program. Hopefully when I am doing the research for these taskings, this is the type of information that is included in documents in the CLI case file.

Once again, thanks for all you do.

[REDACTED]  
SSA [REDACTED]  
Program Manager  
Campus Liaison Initiative

b6  
b7C  
b7E

[REDACTED]  
Counterterrorism Division - FBIHQ

[REDACTED]



Inspection for  
field offices t...



Inspection for  
field offices C...



=====  
Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

b6  
b7C

**From:** [REDACTED] (CTD) (FBI)  
**Sent:** Friday, July 05, 2013 1:45 PM  
**To:** [REDACTED] (SE) (FBI)  
**Subject:** FW: IB-1860: (U) Updated Information Regarding Recent Bomb Threats Against US Aviation and Universities -For Dissem --- UNCLASSIFIED//LES

Classification: UNCLASSIFIED//~~LES~~

=====  
(U) ~~LAW ENFORCEMENT SENSITIVE~~: The information marked (U//~~LES~~) in this document is the property of FBI and may be distributed within the Federal Government (and its contractors), US intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the ~~LES~~ caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked ~~LES~~ on a website or an unclassified network.

Below are the external and internal copies of the IB. You can print and disseminate the EXTERNAL version only.

(the only difference is the on the internal version they list file numbers in the index)

**From:** [REDACTED] (CTD) (FBI)  
**Sent:** Wednesday, July 03, 2013 12:11 PM  
**To:** [REDACTED] (CTD) (FBI)  
**Subject:** FW: IB-1860: (U) Updated Information Regarding Recent Bomb Threats Against US Aviation and Universities - For Dissem --- UNCLASSIFIED//LES

b6  
b7C

Classification: UNCLASSIFIED//~~LES~~

=====  
(U) ~~LAW ENFORCEMENT SENSITIVE~~: The information marked (U//~~LES~~) in this document is the property of FBI and may be distributed within the Federal Government (and its contractors), US intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the ~~LES~~ caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked ~~LES~~ on a website or an unclassified network.

FYI.

**From:** [REDACTED] (DI)(FBI)  
**Sent:** Wednesday, July 03, 2013 12:04 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED] (CTD) (FBI); [REDACTED] (CTD) (FBI); [REDACTED] (CTD) (FBI); [REDACTED] (DI) (FBI); [REDACTED] (CTD) (FBI); [REDACTED] (CTD) (FBI); [REDACTED] (DI) (FBI); [REDACTED] (CTD) (FBI); [REDACTED] (CTD) (FBI); [REDACTED] (DI) (FBI); [REDACTED] (DI) (FBI)

b7E

b6  
b7C



**Subject:** FW: IB-1860: (U) Updated Information Regarding Recent Bomb Threats Against US Aviation and Universities - For Dissem --- UNCLASSIFIED//~~LES~~

Classification: UNCLASSIFIED//~~LES~~

=====

Good Afternoon

Attached is the final external and internal version of **Headquarter IB-1860** for dissemination. The IB, (U) **Updated Information Regarding Recent Bomb Threats Against US Aviation and Universities** was approved by CTD for dissemination.



CTD\_IB1860\_INTE  
RNAL.docx



CTD\_IB1860\_Ext  
ernal.docx

**Band:** VI

**Issue :** All Other Counterterrorism Threats

**KIQs:** ~~(S//NF)~~

b7E

Feel free to contact me if you have any questions or concerns.

Thank You

Writer/Editor  
Production Services Unit

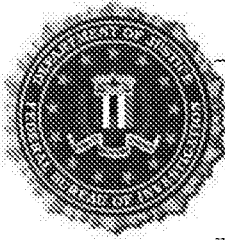
b6  
b7C



=====  
Classification: UNCLASSIFIED//~~LES~~

=====  
Classification: UNCLASSIFIED//~~LES~~





FEDERAL BUREAU OF INVESTIGATION  
INTELLIGENCE BULLETIN  
Counterterrorism Division

3 July 2013

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 02-12-2015 BY NSICG/F76M45K62

(U//~~FOUO~~) [REDACTED]

b7E

(U) ~~LAW ENFORCEMENT SENSITIVE~~: The information marked (U//~~LES~~) in this document is the property of the Federal Bureau of Investigation and may be distributed within the Federal Government (and its contractors), U.S. intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without Federal Bureau of Investigation authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the ~~LES~~ caveat may not be used in legal proceedings without first receiving authorization from the originating agency.

(U//~~LES~~) [REDACTED]

b7E

(U//~~FOUO~~) [REDACTED]

b7E

(U//~~LES~~) [REDACTED]

b7E

<sup>a</sup> (U) See Appendix A for FBI confidence level definitions.

<sup>b</sup> (U) See Appendix B for details on each of the [REDACTED]

b7E



UNCLASSIFIED//~~LAW ENFORCEMENT SENSITIVE~~  
FOR FBI INTERNAL USE ONLY

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Source Summary Statement

(U//FOUO) [REDACTED]

b7E

(U//LES) [REDACTED]

b7E

• (U//LES) [REDACTED]

• (U//LES) [REDACTED]

• (U//LES) [REDACTED]

b7E

• (U//LES) [REDACTED]

10

• (U//LES) [REDACTED]

11, 12

• (U//LES) [REDACTED]

• (U//LES) [REDACTED]

b7E

• (U//LES) [REDACTED]

17

• (U//LES) [REDACTED]

• (U//LES) [REDACTED]

b6  
b7C  
b7E

(U//FOUO) [REDACTED]

b7E

<sup>c</sup> (U//LES) [REDACTED]

<sup>d</sup> (U//FOUO) [REDACTED]

b7E

FOR FBI INTERNAL USE ONLY  
UNCLASSIFIED//~~LAW ENFORCEMENT SENSITIVE~~



~~UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE~~  
FOR FBI INTERNAL USE ONLY

(U) [REDACTED]

b7E

(U//FOUO) [REDACTED]

[REDACTED]

b7E

~~UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE~~

(U//FOUO) [REDACTED]

b7E

(U//TAT) The information in this FBI intelligence bulletin is intended to inform recipients of [REDACTED]

[REDACTED]

**(U) Outlook**

(U//LES) [REDACTED]

b7E

[REDACTED]

**(U) Intelligence Collection Requirements**

(U//FOUO) This intelligence bulletin addresses requirements contained in the FBI National Standing Intelligence Collection Requirements for [REDACTED]

b7E

(U) This product has been prepared by the FBI's [REDACTED] with contributions by the FBI's [REDACTED] Civil Aviation Security Program, Campus Liaison Initiative, Behavioral Analysis Unit, and FBI Divisions in Denver, Los Angeles, Louisville, Newark, Phoenix, Richmond, and San Antonio. Comments and queries may be addressed to the [REDACTED] Unit Chief at [REDACTED]

b6  
b7C  
b7E

<sup>e</sup> (U) A TAT is comprised of professionals trained in conducting a thorough analysis of each incident of threatening communication made toward an organization.



~~UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE~~  
FOR FBI INTERNAL USE ONLY

**(U) Appendix A—FBI Confidence-Level Definitions**

(U) FBI assessments are supported by information that varies in scope, quality and sourcing. Consequently, the FBI ascribes high, medium, or low levels of confidence to judgments as follows:

(U) **High confidence** generally indicates that judgments are based on high-quality information from multiple sources or from a single highly reliable source, or that the nature of the issue makes it possible to render a solid judgment.

(U) **Medium confidence** generally means that the information is credibly sourced and plausible, but can be interpreted in various ways, or is not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.

(U) **Low confidence** generally means that the information's credibility or plausibility is questionable, the information is too fragmented or poorly corroborated to make solid analytic inferences, or that the FBI has significant concerns or problems with the sources.



UNCLASSIFIED//~~LAW ENFORCEMENT SENSITIVE~~  
FOR FBI INTERNAL USE ONLY

(U//~~FOUO~~) Appendix B- [REDACTED]  
[REDACTED]

b7E

(U//~~LES~~) [REDACTED]  
[REDACTED]

b7E

- (U//~~LES~~) [REDACTED]  
[REDACTED]

b7E

- (U//~~LES~~) [REDACTED]  
[REDACTED]

b7E

- (U//~~LES~~) [REDACTED]  
[REDACTED]

b7E

- (U//~~LES~~) [REDACTED]  
[REDACTED]

b7E

- (U//~~LES~~) [REDACTED]  
[REDACTED]

b7E

- (U//~~LES~~) [REDACTED]  
[REDACTED]

b7E

FOR FBI INTERNAL USE ONLY  
UNCLASSIFIED//~~LAW ENFORCEMENT SENSITIVE~~



UNCLASSIFIED//~~LAW ENFORCEMENT SENSITIVE~~  
FOR FBI INTERNAL USE ONLY

[REDACTED]

b7E

- (U//~~LES~~) [REDACTED]

[REDACTED]

b7E

- (U//~~LES~~) [REDACTED]

[REDACTED]

b7E

FOR FBI INTERNAL USE ONLY  
UNCLASSIFIED//~~LAW ENFORCEMENT SENSITIVE~~



~~UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE~~  
FOR FBI INTERNAL USE ONLY

**(U) Endnotes**

<sup>1</sup> (U) FBI; Electronic Communication; [REDACTED] ~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~; UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~; Source is FBI investigative information.

b7E

<sup>2</sup> (U) FBI; Electronic Communication; [REDACTED] ~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~; UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~; Source is FBI investigative information.

<sup>3</sup> (U) FBI; Electronic Communication; [REDACTED] ~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~; UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~; Source is FBI investigative information.

<sup>4</sup> (U) *Ibid.*

<sup>5</sup> (U) *Ibid.*

<sup>6</sup> (U) FBI; Electronic Communication; [REDACTED] UNCLASSIFIED; UNCLASSIFIED; Source is FBI investigative information.

b7E

<sup>7</sup> (U) *Ibid.*

<sup>8</sup> (U) *Ibid.*

<sup>9</sup> (U) *Op. cit.*, endnote 1.

<sup>10</sup> (U) FBI; Electronic Communication; [REDACTED] UNCLASSIFIED; UNCLASSIFIED; Source is FBI investigative information.

b7E

<sup>11</sup> (U) FBI; [REDACTED] (U) [REDACTED] UNCLASSIFIED; UNCLASSIFIED; Multiple underlying sources.

<sup>12</sup> (U) *Op. cit.*, endnote 10.

<sup>13</sup> (U) *Ibid.*

<sup>14</sup> (U) *Ibid.*

<sup>15</sup> (U) *Op. cit.*, endnote 11.

<sup>16</sup> (U) *Ibid.*

<sup>17</sup> (U) *Op. cit.*, endnote 10.

<sup>18</sup> (U) FBI; Internal E-mail from FBI [REDACTED] ~~UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE~~; UNCLASSIFIED//~~LAW ENFORCEMENT SENSITIVE~~; Source is an FBI employee.

b7E

<sup>19</sup> (U) FBI; Electronic Communication; [REDACTED] UNCLASSIFIED; UNCLASSIFIED; Source is FBI investigative information.

<sup>20</sup> (U) *Op. cit.*, endnote 3.

<sup>21</sup> (U) *Op. cit.*, endnote 1.

<sup>22</sup> (U) FBI; Internal E-mail from FBI [REDACTED] ~~UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE~~; UNCLASSIFIED//~~LAW ENFORCEMENT SENSITIVE~~; Source is an FBI employee.

b7E

<sup>23</sup> (U) FBI; Internal E-mail [REDACTED] UNCLASSIFIED; UNCLASSIFIED; Source is an FBI employee.

<sup>24</sup> (U) *Op. cit.*, endnote 6.

<sup>25</sup> (U) *Ibid.*

<sup>26</sup> (U) *Op. cit.*, endnote 11.

<sup>27</sup> (U) *Op. cit.*, endnote 3.

<sup>28</sup> (U) FBI; Electronic Communication; [REDACTED] UNCLASSIFIED; UNCLASSIFIED; Source is FBI investigative information.

b7E

<sup>29</sup> (U) FBI; Electronic Communication; [REDACTED] UNCLASSIFIED; UNCLASSIFIED; Source is FBI investigative information.

<sup>30</sup> (U) *Op. cit.*, endnote 1.

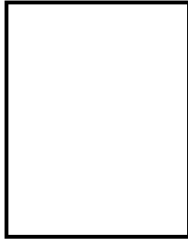
<sup>31</sup> (U) *Op. cit.*, endnote 10.

FOR FBI INTERNAL USE ONLY  
~~UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE~~



UNCLASSIFIED//~~LAW ENFORCEMENT SENSITIVE~~  
FOR FBI INTERNAL USE ONLY

Distribution



b7E

FOR FBI INTERNAL USE ONLY  
UNCLASSIFIED//~~LAW ENFORCEMENT SENSITIVE~~



**UNCLASSIFIED//~~LAW ENFORCEMENT SENSITIVE~~**  
**FOR FBI INTERNAL USE ONLY**

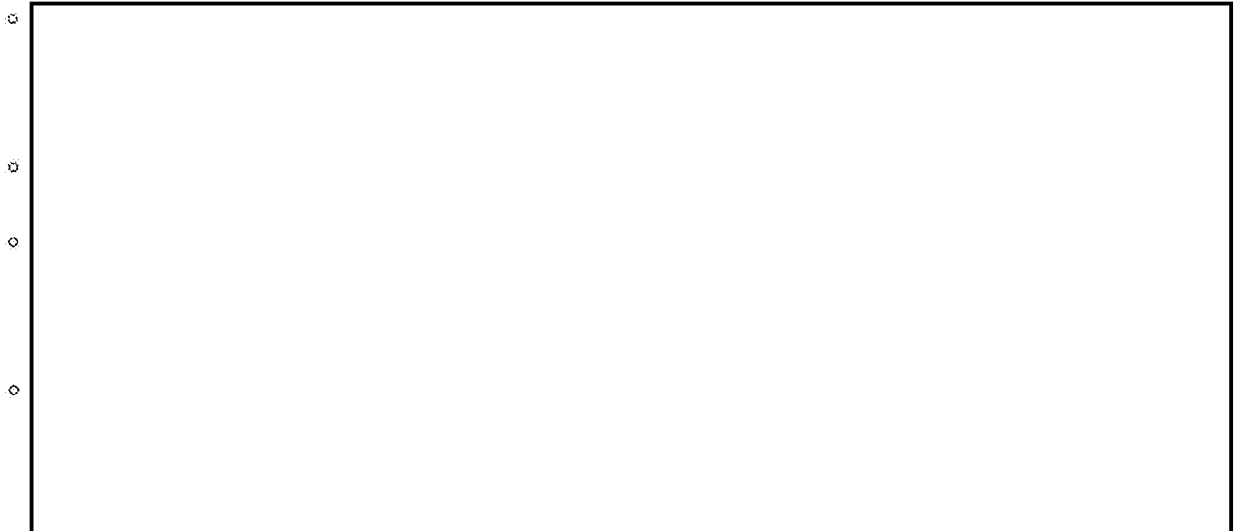
**(U) Library of National Intelligence Instructions**  
**(IDU will detach before dissemination)**

(U) The Library of National Intelligence (LNI) is a central repository of disseminated intelligence products from each IC agency. Pursuant to Intelligence Community Directive (ICD) 501, "*Discovery and Dissemination or Retrieval of Information within the Intelligence Community*," disseminated FBI raw and finished intelligence products shall be posted to the LNI, except those that contain information outside the scope of, or exempted from, the LNI. Refer to ICD 501 for further information.

(U) You must disseminate intelligence products, including those with ORCON and NOFORN dissemination controls, to the LNI unless they meet one of the following exemptions:



b7E





[REDACTED] (RMD)(CON)

From: [REDACTED] (SE) (FBI)  
Sent: Monday, November 10, 2014 6:50 PM  
To: [REDACTED] (RMD)(CON)  
Subject: [REDACTED] -- UNCLASSIFIED//~~FOUO~~

b6  
b7C  
b7E

Follow Up Flag: Follow up  
Flag Status: Flagged  
SentinelCaseId: TRANSITORY RECORD

Classification: UNCLASSIFIED//~~FOUO~~  
ATTORNEY WORK PRODUCT/ATTORNEY-CLIENT PRIVILEGED INFORMATION/DELIBERATIVE  
PROCESS PRIVILEGED DOCUMENT

=====  
TRANSITORY RECORD

Good afternoon [REDACTED]

b5  
b6  
b7C

Take Care,  
[REDACTED]

[REDACTED]  
Supervisory Special Agent  
Chief Division Counsel  
Seattle

b6  
b7C

[REDACTED] main  
[REDACTED] direct

b5  
b7E

=====  
Classification: UNCLASSIFIED//~~FOUO~~



[REDACTED] (RMD)(CON)

From: [REDACTED] (CTD) (OGA)  
Sent: Thursday, June 13, 2013 12:34 PM  
To: [REDACTED] (SE) (FBI)  
Cc: [REDACTED] (CTD) (FBI)  
Subject: [REDACTED] -- UNCLASSIFIED//~~FOUO~~

b6  
b7C  
b7E

Classification: UNCLASSIFIED//~~FOUO~~  
=====

FYSA, the attached [REDACTED]

b6  
b7C  
b7E

(U) [REDACTED]  
[REDACTED]



[REDACTED] b7E

[REDACTED]  
Special Agent  
[REDACTED]  
[REDACTED] Desk

b6  
b7C  
b7E

=====  
Classification: UNCLASSIFIED//~~FOUO~~  
-



[REDACTED] (RMD)(CON)

From: [REDACTED] CTD) (OGA)  
Sent: Wednesday, June 12, 2013 10:59 AM  
To: [REDACTED] (SE) (FBI)  
Cc: [REDACTED] CTD) (FBI); [REDACTED] CTD) (FBI)  
Subject: [REDACTED] UNCLASSIFIED//~~FOUO~~

b6  
b7C  
b7E

Classification: UNCLASSIFIED//~~FOUO~~

FYSA, the attached [REDACTED]

b7E

(U//~~FOUO~~) [REDACTED]

[REDACTED]

b6  
b7C  
b7E

[REDACTED]



[REDACTED]

b7E

(U//~~FOUO~~) [REDACTED]

b7E

Investigative

Method:

Description:

[REDACTED]

[REDACTED]

b6  
b7C  
b7E



[Redacted]

b6  
b7C  
b7E

**Status:** Completed

06/10/2013 02:06:19 PM

**Created Note** [Redacted]

b6  
b7C  
b7E

[Redacted]

( Seattle

/  
Inland Northwest [Redacted] Spokane RA/Richland RA/Yakima RA  
)

[Redacted]

Special Agent

b6  
b7C  
b7E

[Redacted]

[Redacted] Desk

=====  
Classification: UNCLASSIFIED//~~FOUO~~



[REDACTED] (RMD)(CON)

From: [REDACTED] (SE) (FBI)  
Sent: Monday, June 10, 2013 3:40 PM  
To: [REDACTED] (CH) (FBI)  
Cc: [REDACTED] (SE) (FBI)  
Subject: FW: [REDACTED] - UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED

[REDACTED] It doesn't appear that Spokane [REDACTED] has been made aware either, by [REDACTED] given the subject's possible connection/residence in Ellensburg.

b6  
b7C  
b7E

[REDACTED] Do you cover Ellensburg? See below [REDACTED] became aware of this [REDACTED] due to his role as Campus Liaison Agent/Coordinator. It appears the subject [REDACTED], may reside/have a connection to [REDACTED]

b6  
b7C  
b7E

SSA [REDACTED]  
Seattle Division  
Squad CT-1  
[REDACTED] desk  
[REDACTED] cell  
(206) 262-2388 fax  
[REDACTED]

b6  
b7C

From: [REDACTED] (SE) (FBI)  
Sent: Monday, June 10, 2013 12:26 PM  
To: [REDACTED] (SE) (FBI)  
Subject: FW: [REDACTED] --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED

FYI, the [REDACTED] mentioned.

b7E

Haven't seen any leads to me so I assume no follow-up is needed at this time.

From: [REDACTED] (CTD) (OGA)  
Sent: Friday, June 07, 2013 6:40 AM  
To: [REDACTED] (SE) (FBI)  
Cc: [REDACTED] (CTD) (FBI)  
Subject: [REDACTED] --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED



FYSA, the attached [redacted]

b7E

(U) [redacted]

b7E



[redacted]

b7E

[redacted]

b7E

[redacted]

b6  
b7C  
b7E



b6  
b7C  
b7E

[redacted]  
Special Agent

b6  
b7C  
b7E

[redacted]  
[redacted] Desk

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Friday, May 24, 2013 6:17 AM  
**To:** [REDACTED] SE) (FBI)  
**Subject:** RE: Travel Request Form --- UNCLASSIFIED

b6  
b7C  
b7E

Classification: UNCLASSIFIED  
=====

Go ahead and fill out a travel request form that is on our CLI webpage and email a copy to me and I'll take a look at it. I got yelled at yesterday about funding, but I'll see if I can squeeze it in anyway.

**From:** [REDACTED] (SE) (FBI)  
**Sent:** Thursday, May 23, 2013 10:53 AM  
**To:** [REDACTED] CTD) (FBI)  
**Subject:** RE: Travel Request Form --- UNCLASSIFIED

b6  
b7C

Classification: UNCLASSIFIED  
=====

Classic answer. Lol

I haven't had the chance to work with our partners on the East side of our state, like Gonzaga, Eastern Washington, and Washington State, among the myriad community colleges. In talking with one of our SSRA folks out East, a lot of campus partners show up for the [REDACTED] monthly meetings at our Liberty Lake RA and I thought if I spent two days out there I could get some work in for the CLI program. It's really too far for a day trip so I'd need funding.

b7E

Just thinking.

Hope all is well back at LX

**From:** [REDACTED] CTD) (FBI)  
**Sent:** Thursday, May 23, 2013 2:57 AM  
**To:** [REDACTED] SE) (FBI)  
**Subject:** RE: Travel Request Form --- UNCLASSIFIED

b6  
b7C

Classification: UNCLASSIFIED  
=====

Possibly. What are you looking for?

**From:** [REDACTED] (SE) (FBI)  
**Sent:** Wednesday, May 22, 2013 11:43 AM  
**To:** [REDACTED] CTD) (FBI)  
**Subject:** RE: Travel Request Form --- UNCLASSIFIED

b6  
b7C



Classification: UNCLASSIFIED

H [redacted]

Do we still have access to these funds in light of everything going on with our budget?

b6  
b7C

[redacted]  
From: [redacted] (CTD) (FBI)  
Sent: Wednesday, October 10, 2012 9:42 AM  
To: HQ-DIV13-CLA  
Subject: Travel Request Form --- UNCLASSIFIED

Classification: UNCLASSIFIED

CLAs --  
Good news -- CTD has provided the CLI with funding for travel in FY 2013, albeit limited. To partake of these funds, follow the instructions in the CLI Travel SOP document below. The second document is the CLI Travel Request Form which is new for FY13 and must be completed and emailed to me each time. Both documents are located on the CLI website on the Admin page.

<< File: TravelSOP 10-12.docx >> << File: Travel Request Form 10-12.pub >>

The travel funds are eligible to be used in conjunction with campus-related training you provide for your state and local campus public safety partners. The funding allows for your travel to the training (if necessary), along with scheduled speakers and [redacted] members from other field divisions.

b7E

The travel funds should also be utilized to travel to your state or regional campus public safety organizations' training and meetings. These meetings will perpetuate your learning and ensure your awareness of counterterrorism and other issues effecting campuses nationwide. This training will also provide fiscally responsible opportunities for building relationships in one central location with the most significant campus public safety executives in your state or region.

Happy Trails.

[redacted]  
SSA [redacted]  
Program Manager  
Campus Liaison Initiative

b6  
b7C  
b7E

[redacted]  
Counterterrorism Division - FBIHQ  
[redacted]

=====  
Classification: UNCLASSIFIED

=====  
Classification: UNCLASSIFIED



=====

Classification: UNCLASSIFIED

=====

Classification: UNCLASSIFIED

=====

Classification: UNCLASSIFIED



[REDACTED] (RMD)(CON)

From: [REDACTED] (SE) (FBI)  
Sent: Monday, November 10, 2014 6:49 PM  
To: [REDACTED] (RMD)(CON)  
Subject: [REDACTED] - ~~SECRET//NOFORN~~

b6  
b7C  
b7E

Follow Up Flag: Follow up  
Flag Status: Flagged

SentinelCaseId: TRANSITORY RECORD

Classification: ~~SECRET//NOFORN~~

ATTORNEY WORK PRODUCT/ATTORNEY-CLIENT PRIVILEGED INFORMATION/DELIBERATIVE  
PROCESS PRIVILEGED DOCUMENT

Upon removal of attachment(s), this document is UNCLASSIFIED//~~FOUO~~

~~Classified By: C67W98B51  
Derived From: FBI NSIC, dated 20120629  
Declassify On: 20391231~~

=====  
TRANSITORY RECORD

Good afternoon [REDACTED]

b5  
b6  
b7C

Take Care,  
[REDACTED]

[REDACTED]  
Supervisory Special Agent  
Chief Division Counsel  
Seattle

b6  
b7C

[REDACTED] main  
[REDACTED] direct

b5  
b7E

~~SECRET//NOFORN~~  
[REDACTED]

=====  
Classification: ~~SECRET//NOFORN~~



## **EXPLANATION OF EXEMPTIONS**

### **SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552**

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information ( A ) could reasonably be expected to interfere with enforcement proceedings, ( B ) would deprive a person of a right to a fair trial or an impartial adjudication, ( C ) could reasonably be expected to constitute an unwarranted invasion of personal privacy, ( D ) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, ( E ) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or ( F ) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

### **SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a**

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.